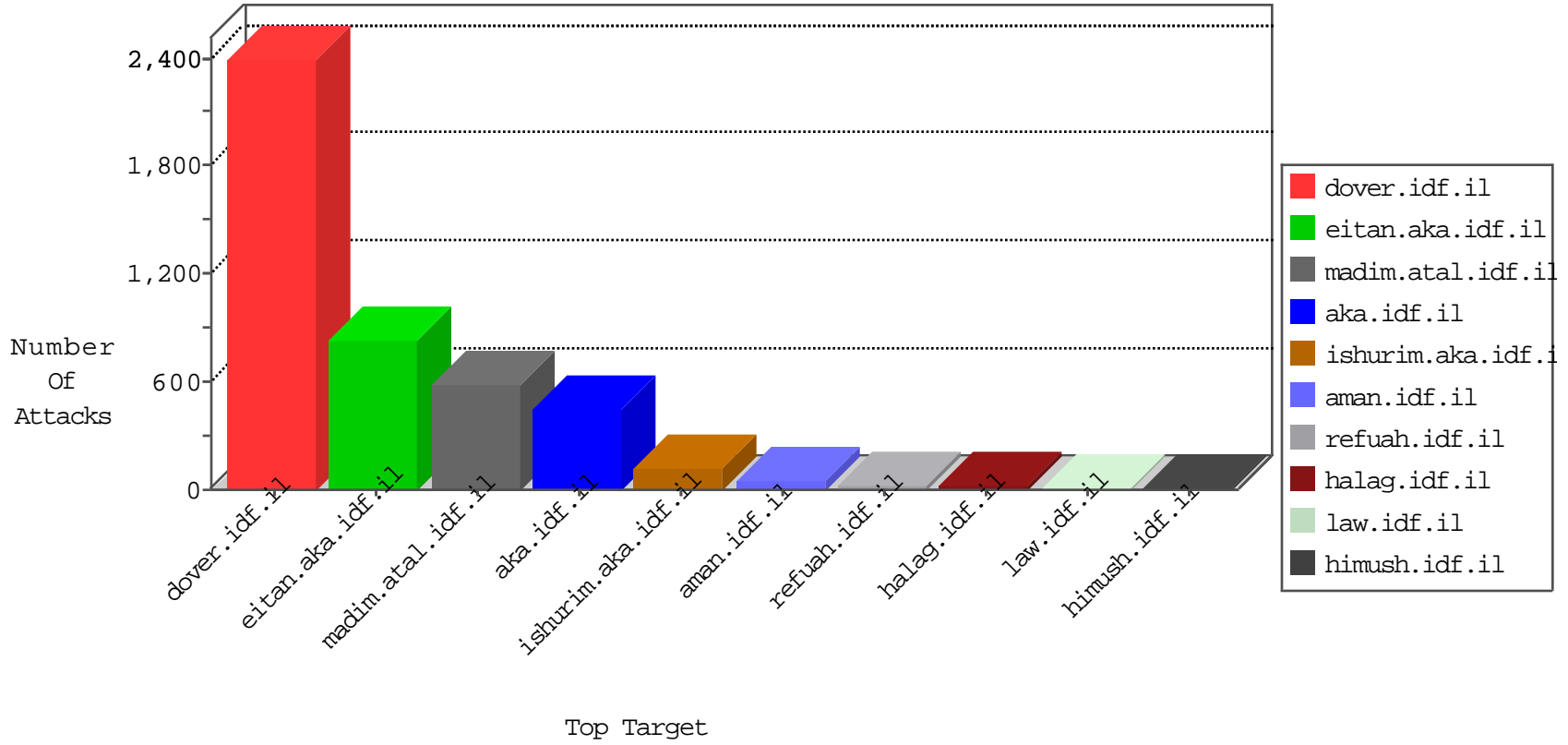


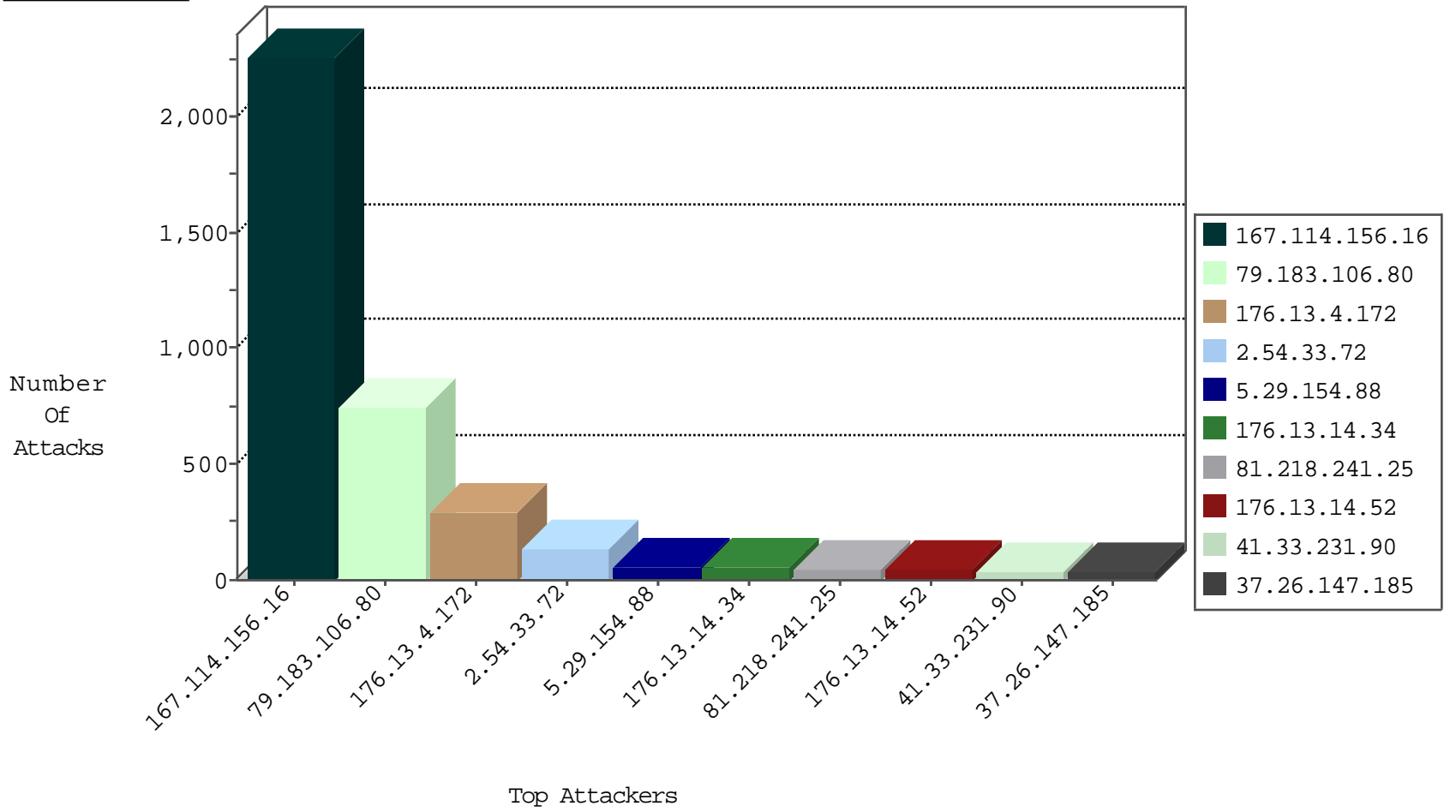
# IDF Under Attack Daily Report



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	3412
81.218.241.25	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	87
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	63
79.178.10.3	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.25.148.67	Germany	147.237.76.31	nakchal.idf.i	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1
52.89.50.240	United States	147.237.77.216	doover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
89.139.171.15	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	11
40.115.58.160	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
218.249.175.229	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -sS window 2048	1
213.151.41.144	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.199.99.132	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.169.251.74	147.237.0.35	Germany	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
62.128.48.50	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.14.94	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.249.175.229	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -f -sS	1
213.8.118.110	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
85.250.111.53	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.207.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.183.106.80	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	639
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
46.19.85.98	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	29
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
46.19.86.201	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	16
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
195.160.240.11	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid sequence number	monitor	13
83.130.99.188	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
83.130.99.188	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
81.218.241.25	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	11
5.29.154.88	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
80.179.225.170	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
109.64.154.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
185.120.126.40		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.253	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
81.218.241.25	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.155	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.97	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.49	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.181.218.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
147.236.34.135	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
109.66.174.176	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.193	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.49	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.148.168	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
207.241.226.109	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	6
79.182.129.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.231	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.146.178	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.54.170	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
213.57.134.79	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.225	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
213.57.134.79	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
82.166.93.161	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	5
46.19.86.144	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
91.200.12.137	Ukraine	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	4
79.183.178.53	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
79.182.34.214	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
91.200.12.137	Ukraine	147.237.77.233	atal.idf.il	drop	SAM rule	drop	4
46.19.85.135	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.146.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.128	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.239	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.23.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.27.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
37.19.116.218	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.33.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	136
176.13.4.172	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 176.13.4.172	Block	134
176.13.4.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	128
79.183.106.80	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	107
176.13.14.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
5.29.154.88	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	46
176.13.14.52	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	44
37.26.147.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
46.19.86.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
176.13.4.172	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 176.13.4.172	Block	25
176.13.5.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
62.219.193.62	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 62.219.193.62	Block	11
176.13.18.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
62.219.211.64	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authentication-service.aspx/getauthuser	Block	6
46.19.85.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/\$\$\$&?&?\$\$\$	Block	3
89.138.69.208	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 89.138.69.208	Block	3
37.26.147.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.64.62.145	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	3
37.26.147.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
149.78.251.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
84.95.252.40	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	2
46.19.86.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
89.138.69.208	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	2
46.121.203.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.235.13.100	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
89.138.72.188	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/default.asp	Block	2
91.121.83.118	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
185.120.125.55		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.121.85.136	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.94.119.247	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized Method POST for www.chinuch.aka.idf.il/900-he/chinuch.aspx	None	1
79.182.24.18	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.85.191	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
176.12.148.49	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.79.12	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/938-he/nakchal.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
37.26.147.205	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
2.54.178.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.250.206.244	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
62.90.100.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/x?x™x@x•x™x?	Block	1
184.105.139.67	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
46.19.21.106	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
146.185.56.54	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
79.179.119.163	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
213.57.182.173	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20191-he/dover.aspx	Block	1
195.154.226.90	France	147.237.72.166	aka.idf.il	Illegal HTTP Version HTTP/	Block	1
37.19.116.218	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
91.121.83.118	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1