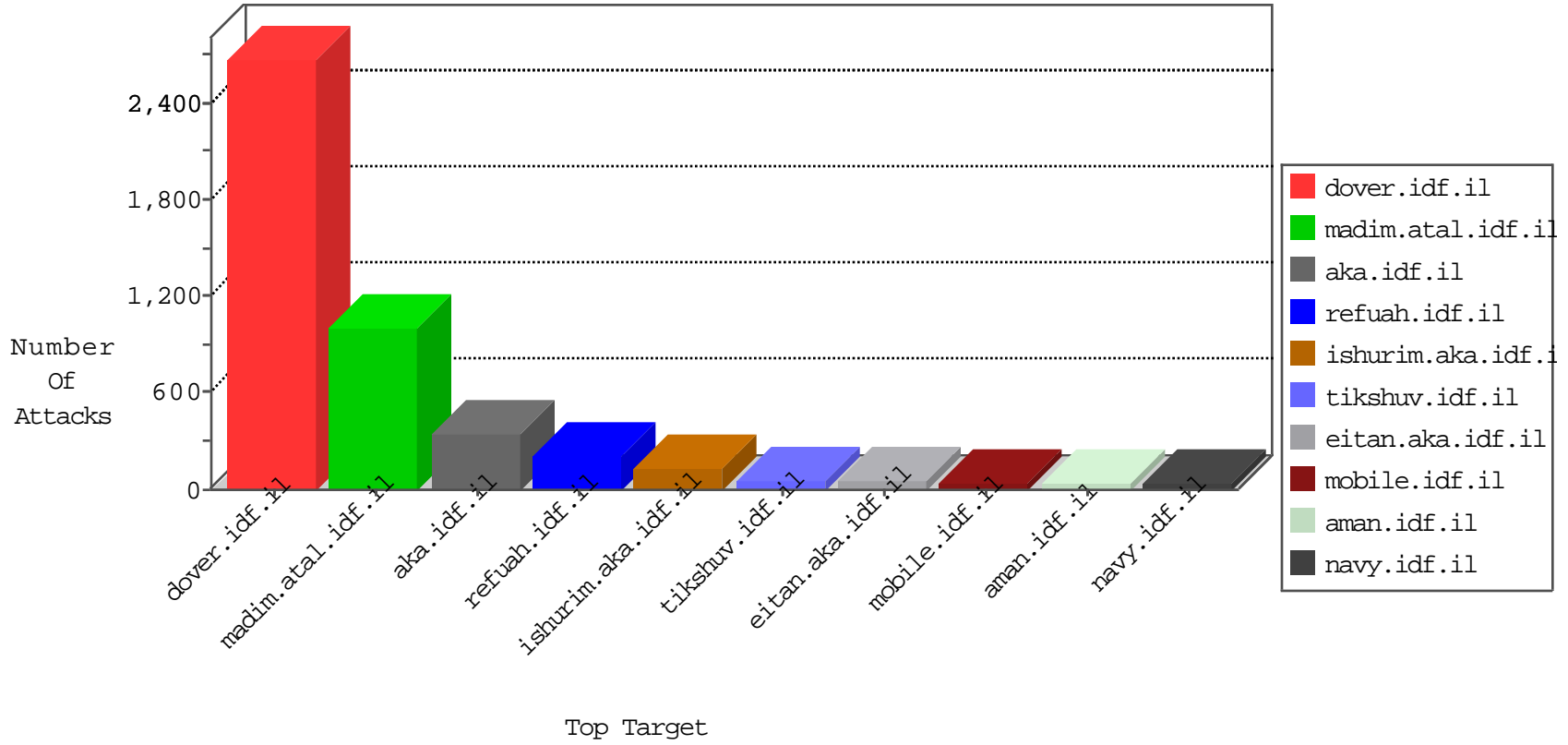


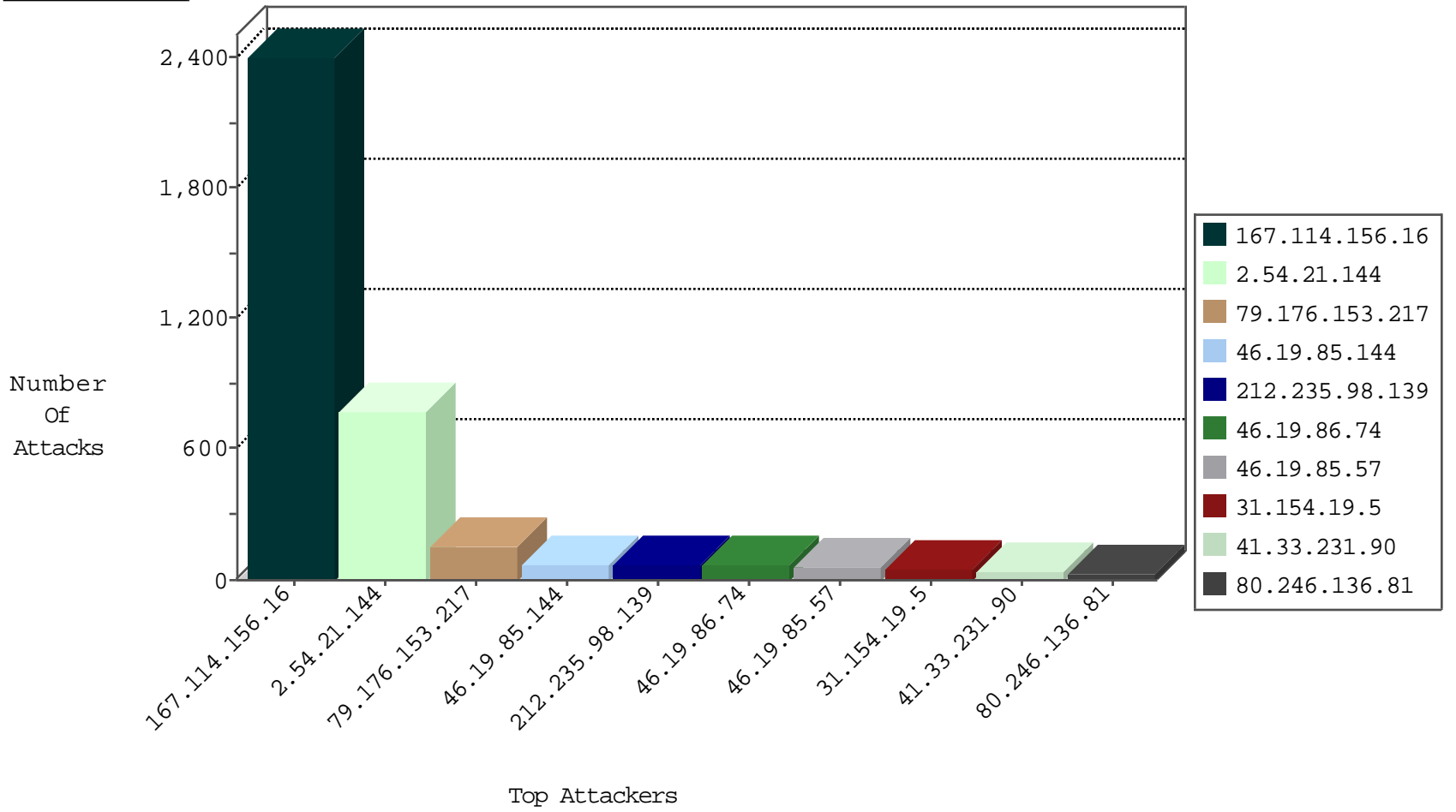
IDF Under Attack Daily Report



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	3623
82.166.137.19	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	234
82.81.12.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
212.179.177.148	Israel	147.237.72.166	aka.idf.il	block-sp-trafl	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.154	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
188.165.15.105	France	147.237.72.156	aman.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.119	France	147.237.76.31	nakchal.idf.il	C228: HTTP: AhrefBot crawler	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	3
2.52.134.31	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	3
84.108.74.28	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.68.78	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.39.222.253	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
2.52.134.95	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.59.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.235.254.181	147.237.76.34	Turkey	yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
94.102.48.195	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
79.180.225.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.39.222.253	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
5.22.134.120	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.235.79.14	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
112.196.49.101	147.237.76.148	India	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 4096	1
109.66.202.155	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.77.176	Netherlands	matpash.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
79.176.153.217	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	148
46.19.85.57	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	53
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
80.246.136.81	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	29
37.26.146.234	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	21
217.194.195.141	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	19
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
80.246.137.64	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
162.243.103.236	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
46.19.86.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
84.228.144.160	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.180.225.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.12.147.160	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
125.88.8.235	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
81.218.251.250	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
93.172.133.247	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
31.154.19.5	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.142.210	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.3.146.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.8.59.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.163.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.41.50	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
212.179.21.194	Israel	147.237.76.177	ncore.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.81.50.145	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.39.215	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.23.54	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.195.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.246	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.80	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
94.230.86.241	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.80	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.179.224.186	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
147.236.38.29	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
176.12.147.160	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.196	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.246	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.123	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.3.146.249	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.180.22.38	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
176.12.147.160	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.193	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.30	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
185.3.146.251	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.150.195.192	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.30	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.21.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	494
2.54.21.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	177
2.54.21.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	98
46.19.85.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
46.19.86.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	64
31.154.19.5	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	40
2.54.50.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
176.13.20.72	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
46.19.86.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
176.13.15.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	11
46.19.86.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
80.246.137.64	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
109.253.159.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.85.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.41.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
162.243.103.236	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 162.243.103.236	Block	3
212.235.98.139	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.235.98.139	Block	3
2.54.54.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
149.78.228.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
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	2
46.19.86.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.64.7.93	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
198.1.127.179	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 198.1.127.179	Block	2
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.15.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.23.54	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
212.199.169.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.108.124.49	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/kapatz/undefined	Block	2
95.86.85.156	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 95.86.85.156	Block	2
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	2
2.54.7.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.80.17.163	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.17.219	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
37.26.147.172	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
79.180.220.251	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/adguard-ajax-api/injections/web of trust	Block	1
212.179.177.148	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
2.54.41.223	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.184	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 5cf35968 in aka.idf.il/news/	None	1
212.179.177.148	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
192.114.105.254	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.17.59	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.64.3.144	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
213.57.151.123	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.6.80	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.177.109.65	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.179.177.148	Israel	147.237.72.166	aka.idf.il	Malformed URL [[#20]]h*	Block	1
2.54.156.58	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.67.164.140	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.86.85.156	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/7/	Block	1
52.48.69.17	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1