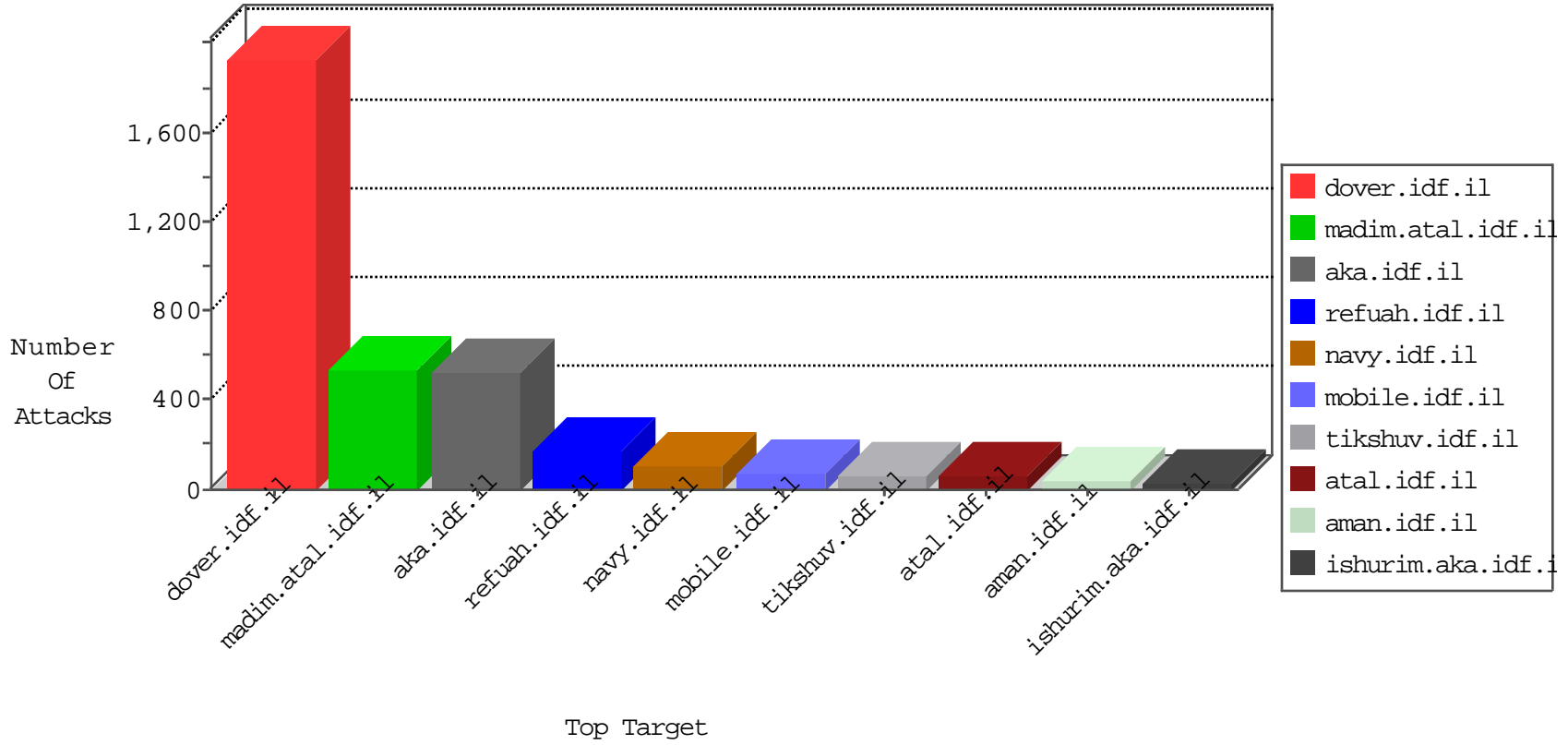


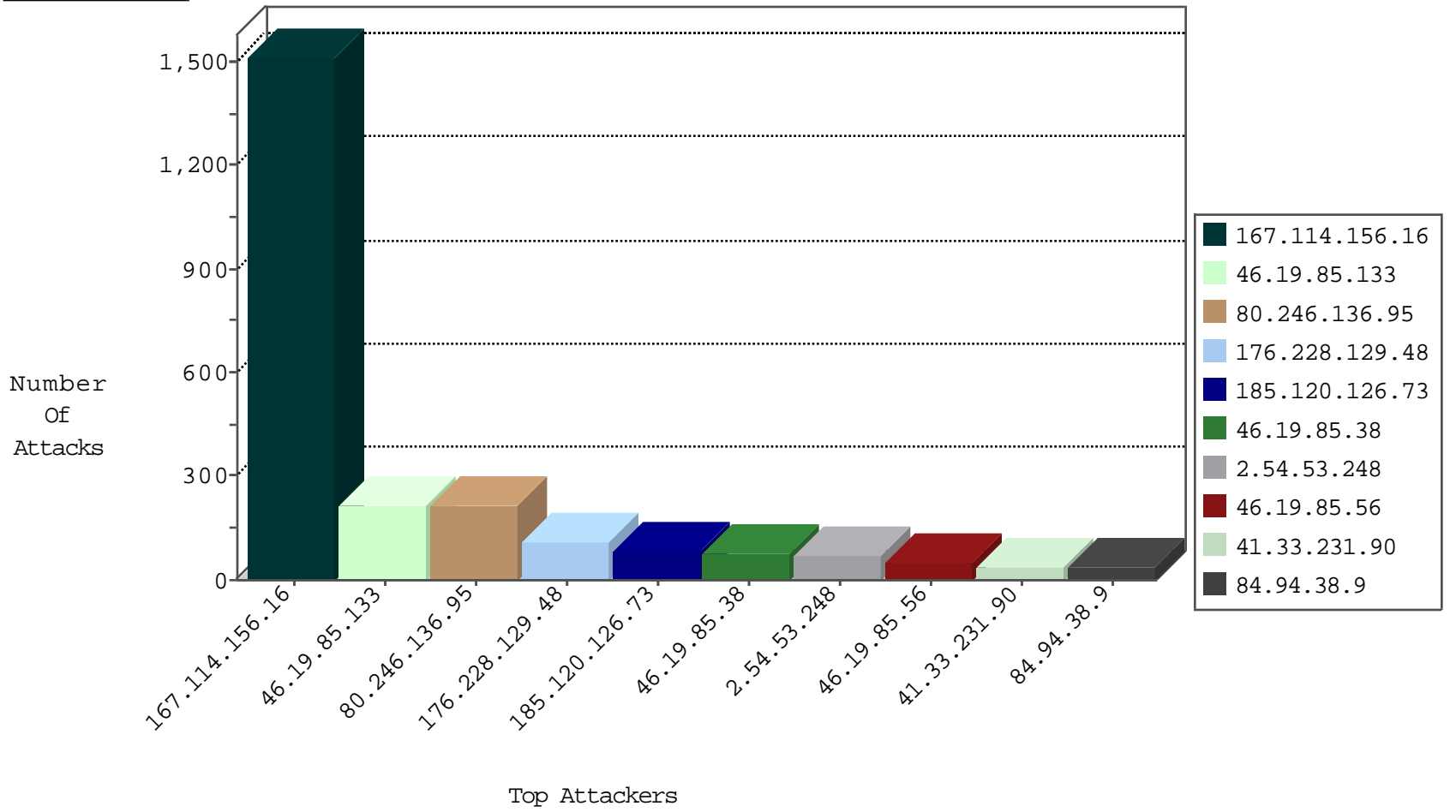
IDF Under Attack Daily Report



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	3228
79.179.139.183	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
212.29.194.254	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
71.6.165.200	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
172.245.128.159	United States	147.237.77.216	dover.idf.i	19813: HTTP: WordPress Theme Divi Directory Traversal Vulnerability	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	2
82.166.236.73	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
77.125.134.65	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.102.9.13	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
167.88.9.227	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
111.85.219.12	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
111.85.219.12	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
111.85.219.12	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.203	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
89.163.209.190	147.237.76.177	Germany	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
79.183.162.9	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.203.215.1	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.249.73.198	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
186.125.137.124	147.237.77.216	Argentina	dover.idf.il	portscan: TCP Distributed Portscan	1
141.212.122.160	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
111.85.219.12	147.237.77.205	China	prisha.idf.il	ET SCAN Potential SSH Scan	1
111.85.219.12	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
108.104.153.115	147.237.76.201	United States	e.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.174.93.203	147.237.76.196	Netherlands	e.sviva.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
176.228.129.48	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	107
185.120.126.73		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	55
2.54.53.248	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
185.120.126.73		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	28
107.167.104.163	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	27
46.120.201.129	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
192.0.81.57	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	22
80.246.139.23	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	14
62.0.217.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
2.52.172.152	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.176.143.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
208.115.111.68	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	12
46.19.85.38	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.38	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
46.19.85.38	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
46.19.85.38	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	9
192.117.167.66	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.38	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
41.34.42.182	Egypt	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	9
197.211.53.13	Nigeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.86.39	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.52.30.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.38	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
2.54.53.248	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
2.54.53.248	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.54.53.248	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
46.19.85.38	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
46.19.86.172	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
192.0.80.167	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
46.19.85.38	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
109.253.142.153	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
109.253.142.153	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.14.177	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.86.142	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.86.18	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.215	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.70	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.205	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.70	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.49	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.92	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
95.86.105.102	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.139	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
176.13.4.123	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.49	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.70	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.4.123	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.95	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	110
46.19.85.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	110
46.19.85.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	93
80.246.136.95	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	57
46.19.85.56	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	52
84.94.38.9	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	35
80.246.136.95	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	31
80.246.136.95	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	19
37.26.146.184	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	17
216.72.40.185	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
46.19.86.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	16
46.19.85.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	14
109.253.206.55	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.19.129	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.117	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
80.246.137.135	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	3
176.13.1.167	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.179.121.169	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	3
80.246.138.99	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.147.229	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.111.187.38	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
2.54.43.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.26	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
81.218.251.252	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	2
85.64.240.228	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	2
84.111.190.247	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	2
80.179.19.179	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
87.69.170.120	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/www.tikshuv.idf.il	Block	2
46.19.86.117	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
79.179.121.169	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 79.179.121.169	Block	2
109.253.209.160	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.22.219	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
213.151.50.163	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 213.151.50.163	Block	2
37.26.146.141	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.39.206	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.186.55.51	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	2
66.249.78.158	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
84.111.190.247	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.111.190.247	Block	1
37.153.230.235	Netherlands	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/arabic/pages/default.aspx	Block	1
80.178.97.63	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.13.1.13	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
79.179.6.81	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.86.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.108.207.32	Israel	147.237.72.166	aka.idf.il	Distributed Malformed HTTP Header Line	Block	1
209.88.198.1	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/sip_storage/files/7	Block	1
2.54.50.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.176.143.226	Israel	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	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
46.19.86.24	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.115.248.2	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1