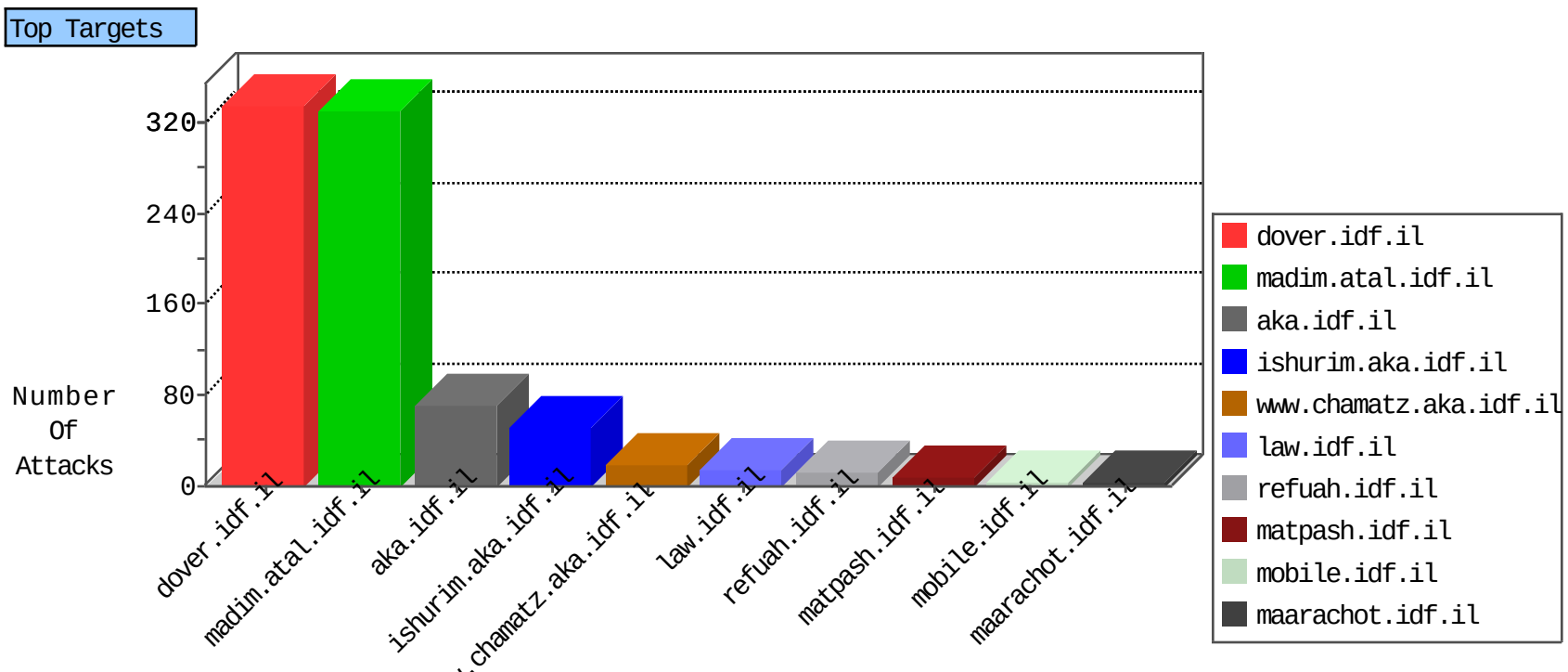
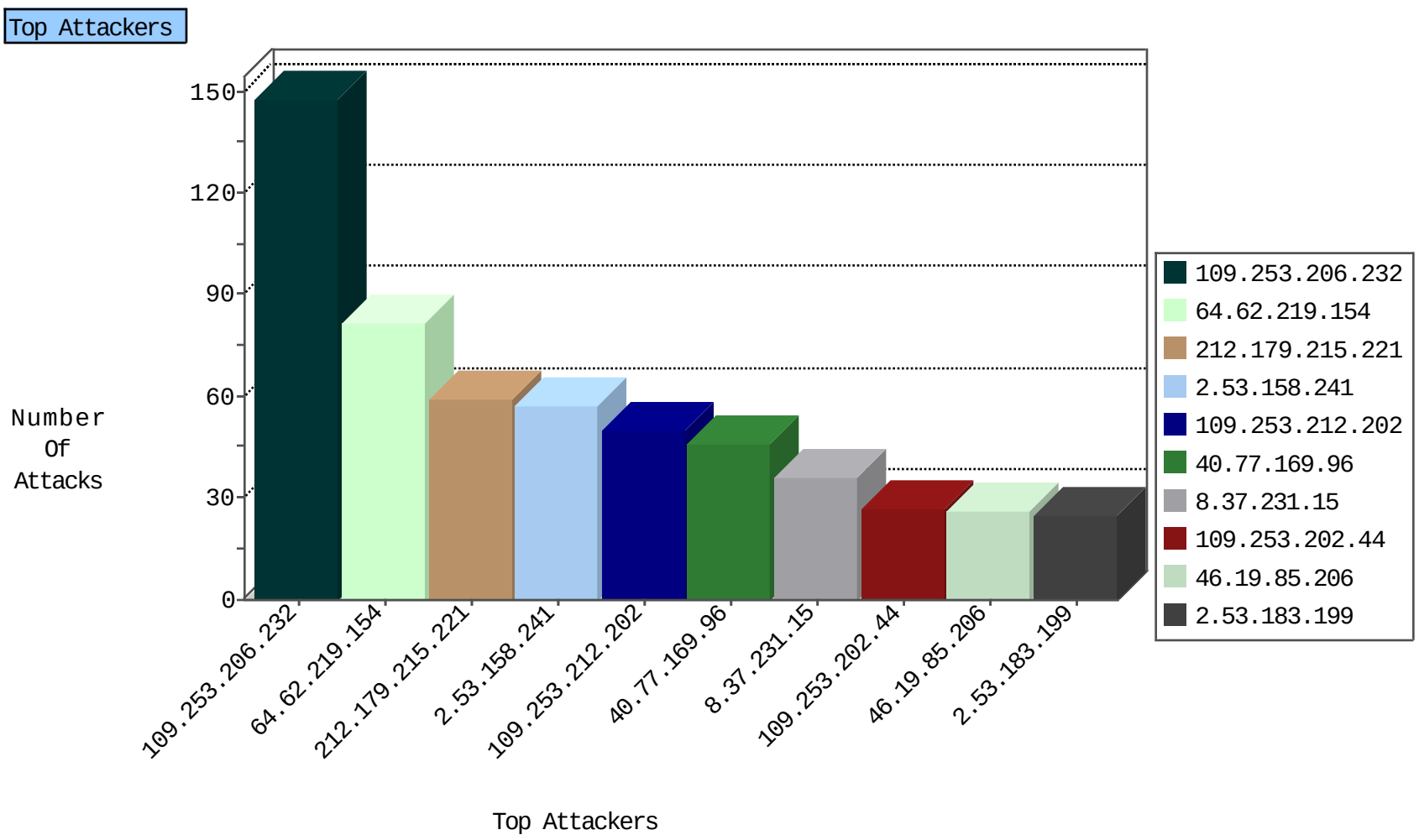
08-24-2016-12:04:08 to 08-24-2016-13:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-24-2016-12:04:08 to 08-24-2016-13:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
8.37.231.15	United States	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	479
8.37.231.15	United States	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	forward	61
109.253.202.44	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	27
84.229.33.145	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
109.66.17.224	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
217.132.145.74	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
79.178.4.197	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
84.108.61.181	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
79.178.155.192	Israel	147.237.72.166	aka.idf.il	Black List	drop	3
79.178.155.192	Israel	147.237.77.216	dover.idf.il	Black List	drop	3
79.179.11.235	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
46.121.211.254	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
77.138.102.232	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
209.126.136.2	United States	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
212.179.215.221	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

08-24-2016-12:04:08 to 08-24-2016-13:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.242.112.35	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
23.91.70.95	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
87.242.112.35	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
23.91.70.42	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
23.91.70.46	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
144.76.29.66	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
89.163.148.22	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	1
89.163.148.22	Germany	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	1
89.163.148.22	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	1
1.179.134.194	Thailand	147.237.77.216	dover.idf.il	13076: HTTP: Apache Struts 2 OGNL Command Injection Vulnerability	Block	1
123.125.125.184	China	147.237.76.200	eitan.aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
89.138.128.253	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

08-24-2016-12:04:08 to 08-24-2016-13:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
217.132.3.72	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
109.65.15.111	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.138.197.229	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.0.102.190	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.108.29	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
178.220.165.231	147.237.76.177		ncore.idf.il	ET SCAN NMAP -sS window 4096	1
95.211.191.158	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
77.124.19.131	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

08-24-2016-12:04:08 to 08-24-2016-13:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
64.62.219.154	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	77
212.179.215.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
185.89.85.25	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
212.199.34.114	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	12
40.77.169.96	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	12
109.253.135.120	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
178.215.221.63	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
82.166.140.117	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.179.215.221	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
109.253.220.202	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
87.70.6.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
62.0.212.225	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	6
144.15.240.8	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
64.62.219.154	United States	147.237.77.216	dover.idf.il	drop		drop	5
85.130.130.150	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	4
217.132.35.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
178.215.221.63	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
62.128.48.84	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.179.215.221	Israel	147.237.76.147	chinuch.aka.idf.il	drop	First packet isn't SYN	drop	2
79.178.177.182	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.118.10.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
8.37.231.15	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.241.236	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	2
100.92.117.4		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.226.164.96	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.245.225	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
79.178.4.197	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
185.120.125.24	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	2
109.253.212.202	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	1
190.183.60.253	Argentina	147.237.76.34	yohalan.idf.il	drop		drop	1
176.13.2.10	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
46.19.86.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.238.119	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
100.92.51.83		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
184.105.139.124	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
139.162.37.147	United States	147.237.0.33	idf.il	drop		drop	1
84.108.61.181	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
77.138.102.232	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
212.199.34.114	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	1
31.154.49.49	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
85.64.24.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.206.232	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	148
2.53.158.241	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	57
109.253.212.202	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	49
46.19.85.206	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	26
2.53.183.199	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	25
46.19.85.107	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
40.77.169.99	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
80.246.138.50	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.14.195	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
77.139.78.157	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
2.55.145.126	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.53.9.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.225.100	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
64.62.219.84	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
40.77.169.100	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
40.77.169.96	United States	147.237.77.176	matpash.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
40.77.169.101	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
167.220.232.104	Japan	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
40.77.169.98	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
77.138.210.22	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.179.215.221	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
66.249.64.163	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1770	Block	1
46.121.243.222	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.211.208	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
40.77.169.102	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
79.183.39.59	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.75.75	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-21713-he/idfgdover.aspx	Block	1
31.173.39.89	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
64.62.219.158	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
81.218.56.171	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/shared/mailthisclose.png	Block	1
40.77.169.99	United States	147.237.77.74	law.idf.il	Illegal Byte Code Character in URL /351-en/patzar.aspx#011404	Block	1
212.199.118.19	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 212.199.118.19	Block	1
66.249.66.182	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/5/2685.jpg	Block	1
64.62.219.76	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
80.246.130.145	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/scroller/skin.css	Block	1
40.77.169.104	United States	147.237.77.234	halag.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
37.8.33.120	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	1
64.62.219.163	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
93.173.239.208	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.19.86.209	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
77.139.116.235	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	1
5.102.242.218	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.199.118.19	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/trigger.png	Block	1
66.249.66.185	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
147.236.238.41	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	1
80.246.130.165	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/datepicker.css	Block	1
46.19.85.37	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
40.77.169.96	United States	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1