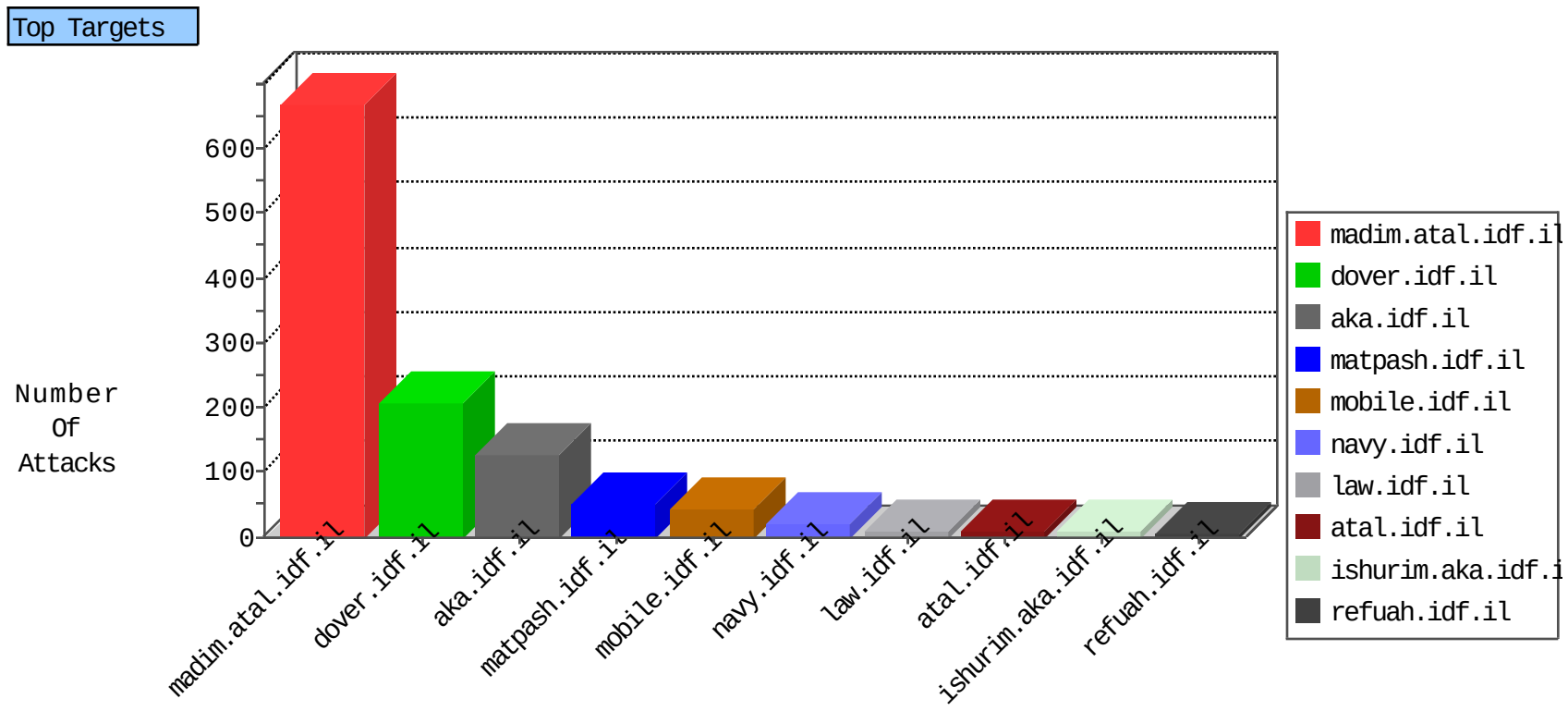
01-28-2016-07:04:07 to 01-28-2016-08:04:07

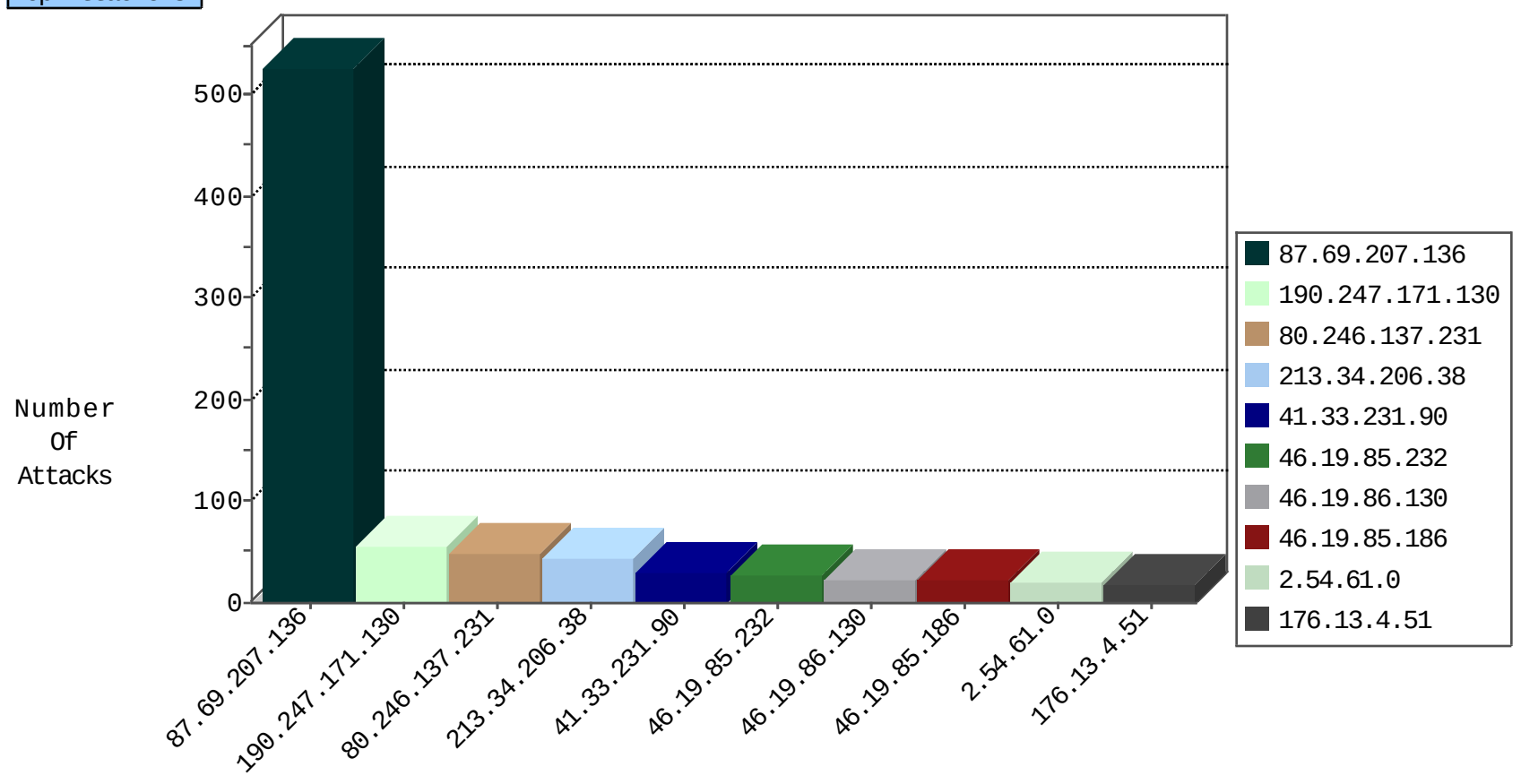
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-28-2016-07:04:07 to 01-28-2016-08:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
104.233.110.79		147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
104.233.110.79		147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
61.160.224.129	China	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
104.233.110.79		147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1

01-28-2016-07:04:07 to 01-28-2016-08:04:07

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

01-28-2016-07:04:07 to 01-28-2016-08:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
213.156.114.84	147.237.0.15	Poland	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
192.157.230.108	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	1
119.246.92.177	147.237.0.33	Hong Kong	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
88.249.106.23	147.237.77.74	Turkey	law.idf.il	ET SCAN NMAP -sS window 1024	1
66.240.213.93	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
175.6.228.149	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Rapid POP3 Connections - Possible Brute Force Attack	1
114.112.90.54	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
84.111.158.134	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.161.40.120	147.237.8.46	Russian Federation	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1

01-28-2016-07:04:07 to 01-28-2016-08:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
213.34.206.38	Kuwait	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	43
190.247.171.130	Argentina	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	30
2.54.61.0	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
46.19.85.232	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
66.249.65.251	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
46.19.85.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
62.219.228.23	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
207.232.27.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.146.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
194.114.146.227	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
80.179.114.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.67	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
47.20.227.179	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.19.52	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.125	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.85.125	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
190.247.171.130	Argentina	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
2.54.4.219	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
176.13.3.173	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.168.16.94	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
207.46.13.49	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.137	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.245	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
80.246.136.146	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.224.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.58	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.123.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.132.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.81.6.33	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
187.189.195.40	Mexico	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
158.116.225.43	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.206.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
190.247.171.130	Argentina	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
188.120.148.130	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
31.210.186.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.3.173	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.85.11	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
5.22.131.5	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
51.254.141.254	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
80.178.138.115	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.85.116	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
109.73.127.69	United Kingdom	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
87.69.207.136	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 87.69.207.136	Block	307
87.69.207.136	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 87.69.207.136	Block	115
87.69.207.136	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	104
80.246.137.231	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	48
46.19.86.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	23
46.19.85.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
176.13.4.51	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
80.246.136.75	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
190.247.171.130	Argentina	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 190.247.171.130	Block	7
176.13.6.84	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
85.65.127.79	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 85.65.127.79	Block	3
80.246.138.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.213.121	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	3
213.151.32.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
149.78.23.128	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.27	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
190.247.171.130	Argentina	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 190.247.171.130	Block	3
82.166.140.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.160	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.66.53.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.137	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
188.143.232.15	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.15	Block	2
80.246.136.178	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.198.151.37	Europe	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$btnSubmit.x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.78.239	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/templates/shared/usercontrols/navmenu/	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
46.19.86.69	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
31.168.16.94	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 31.168.16.94 (Open Mode)	None	1
188.143.232.15	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/homepage.aspx/templates/social/twitter.aspx	Block	1
72.252.202.42	Jamaica	147.237.77.74	law.idf.il	eMail Hoarding	Block	1
51.254.141.254	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
156.198.121.189		147.237.77.216	dover.idf.il	PHP Attempt	Block	1
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docid in www.aka.idf.il/main/giyus/general.aspx	None	1
176.13.19.52	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.19.86.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.168.16.94	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
72.252.202.42	Jamaica	147.237.77.176	matpash.idf.il	E-mail collector robots 14	Block	1
54.243.53.148	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1283-12386-en/dover.aspx	Block	1
156.198.121.189		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
2.54.130.144	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
178.255.215.87	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/aman	Block	1
40.77.167.20	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/robots.txt	Block	1
85.65.127.79	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
190.247.171.130	Argentina	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
72.252.202.42	Jamaica	147.237.77.176	matpash.idf.il	eMail Hoarding	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-17516-he/dover.aspx	Block	1
157.55.39.224	United States	147.237.72.166	aka.idf.il	Unknown Parameter 136cd360 in www.aka.idf.il/main/home/default.aspx	None	1