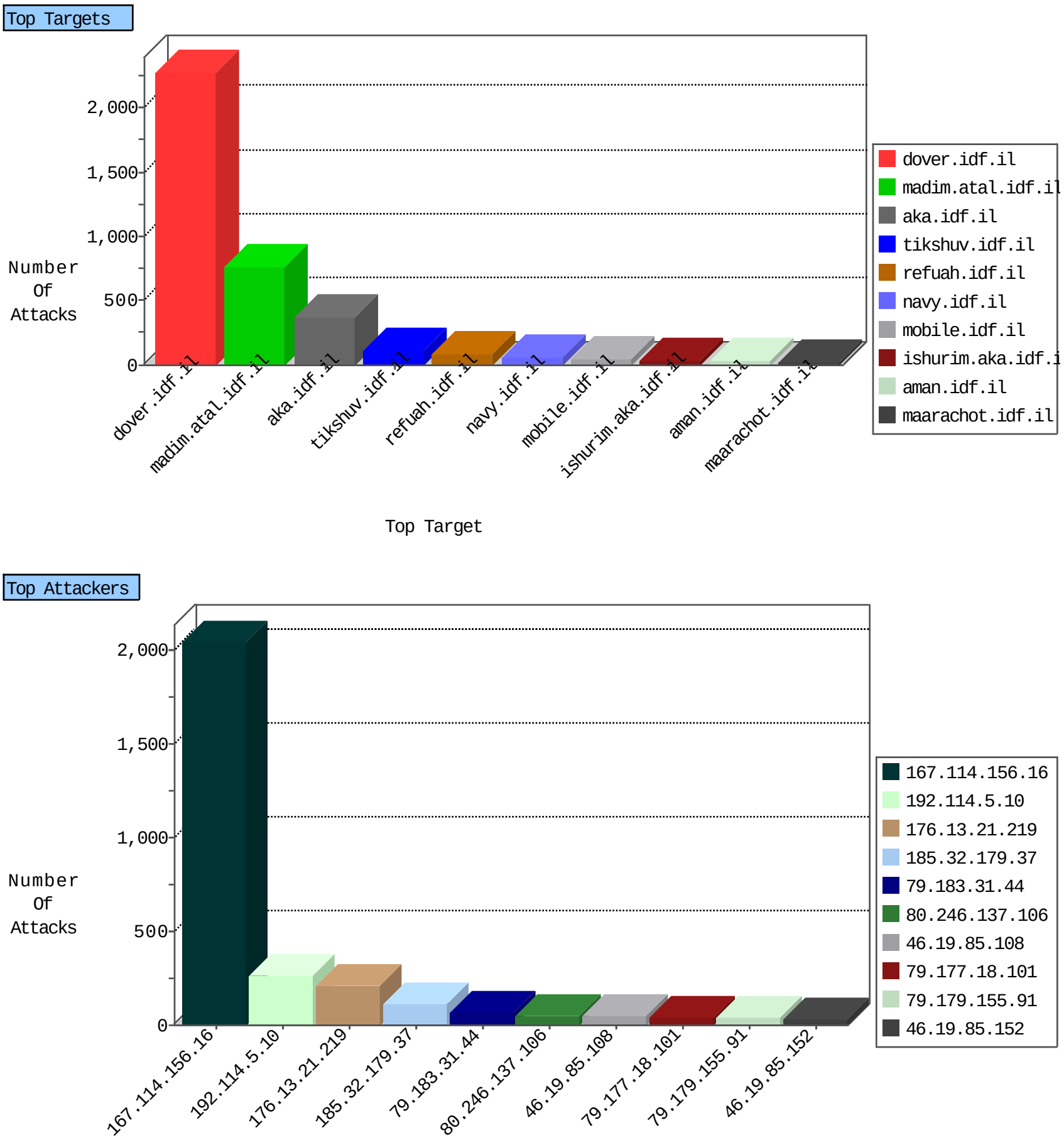
01-13-2016-18:04:06 to 01-13-2016-19:04:06

IDF Under Attack Daily Report



01-13-2016-18:04:06 to 01-13-2016-19:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.73.206	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	3237
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3061
79.182.212.253	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
71.6.165.200	United States	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

01-13-2016-18:04:06 to 01-13-2016-19:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
216.17.111.245	United States	147.237.77.226	www.chamatz.aka.idf.il	16634: HTTP: Apache HTTP Server mod_status Request	Block	1

01-13-2016-18:04:06 to 01-13-2016-19:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
194.114.146.227	147.237.72.167	Israel	ishurim.aka.idf.i	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
84.109.192.59	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.82.79.104	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
37.142.64.98	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
197.157.244.243	147.237.77.216	Somalia	dover.idf.il	ET SCAN Potential SSH Scan	1
2.52.7.151	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.0.200	China	m4u.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
109.67.21.175	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
106.38.241.106	147.237.72.166	China	aka.idf.il	portscan: TCP Distributed Portscan	1
84.228.44.45	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.81.5.3	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.224	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.178.252	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.120.125.53	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
176.228.216.141	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.193.129	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
98.82.54.39	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1

01-13-2016-18:04:06 to 01-13-2016-19:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.183.31.44	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	34
79.183.31.44	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
79.178.34.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
79.179.155.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
79.179.155.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
95.27.188.24	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
79.182.111.254	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
2.52.34.62	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
79.180.51.23	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
176.13.4.2	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.85.187	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
5.102.253.55	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.52.134.207	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.22	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.124	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.204	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
85.250.236.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.204	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.133.209	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
173.252.89.56	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
31.168.72.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.189	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.41	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
198.204.249.34	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.181.243.149	Finland	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.204	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.176.61.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.189	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
85.250.236.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
213.8.114.85	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.181.243.149	Finland	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.183.36.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
173.252.89.53	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
85.130.139.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.136.74	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
85.130.139.95	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
79.181.201.243	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
94.230.86.211	Israel	147.237.76.39	mobile.meitav.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.17	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.17	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
62.0.200.169	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	5
109.66.194.56	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.3.144.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.17	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
180.180.122.22	Thailand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.54.136.14	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.114.5.10	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 192.114.5.10	Block	133
192.114.5.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	129
185.32.179.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	113
176.13.21.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	109
176.13.21.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	99
80.246.137.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
79.177.18.101	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 79.177.18.101	Block	43
46.19.85.108	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	41
46.19.85.152	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
80.246.136.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
176.13.5.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
80.246.137.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
46.19.86.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
46.19.86.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
2.54.144.173	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 2.54.144.173	Block	8
188.143.232.19	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.19	Block	7
208.115.113.88	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/giyus/forum/asp/showforum.asp	Block	7
84.228.29.54	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/resource/userfollowresource/create/	Block	4
17.138.57.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	4
46.200.35.165	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim/resources/images/body/images/main.jpg	Block	4
176.13.4.2	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
80.246.136.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.222.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.8.114.85	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	2
79.180.177.114	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
17.138.57.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
84.94.161.14	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
192.116.247.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/	Block	2
46.19.86.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.21.177	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.13.21.177	None	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
185.32.179.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	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
79.179.155.91	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
5.29.178.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
77.247.181.162	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
184.168.200.28	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
31.168.14.82	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
93.115.95.204	Anonymous Proxy	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19597-he/dover.aspx	Block	1
2.54.144.173	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/g	Block	1
84.108.69.53	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.136.2	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
195.64.164.134	France	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
46.19.86.229	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.192.195	Israel	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.179.168.80	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
5.102.253.55	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1