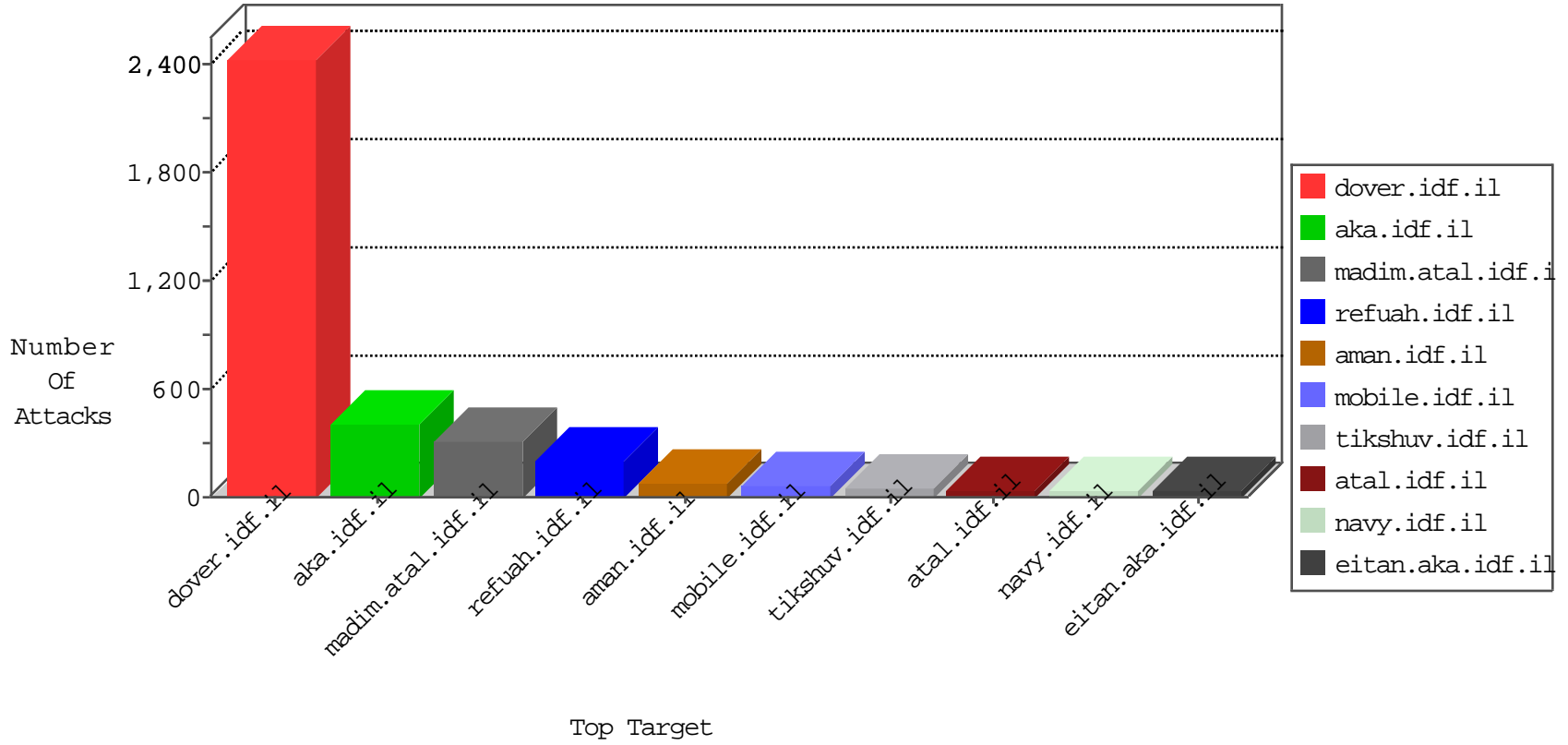


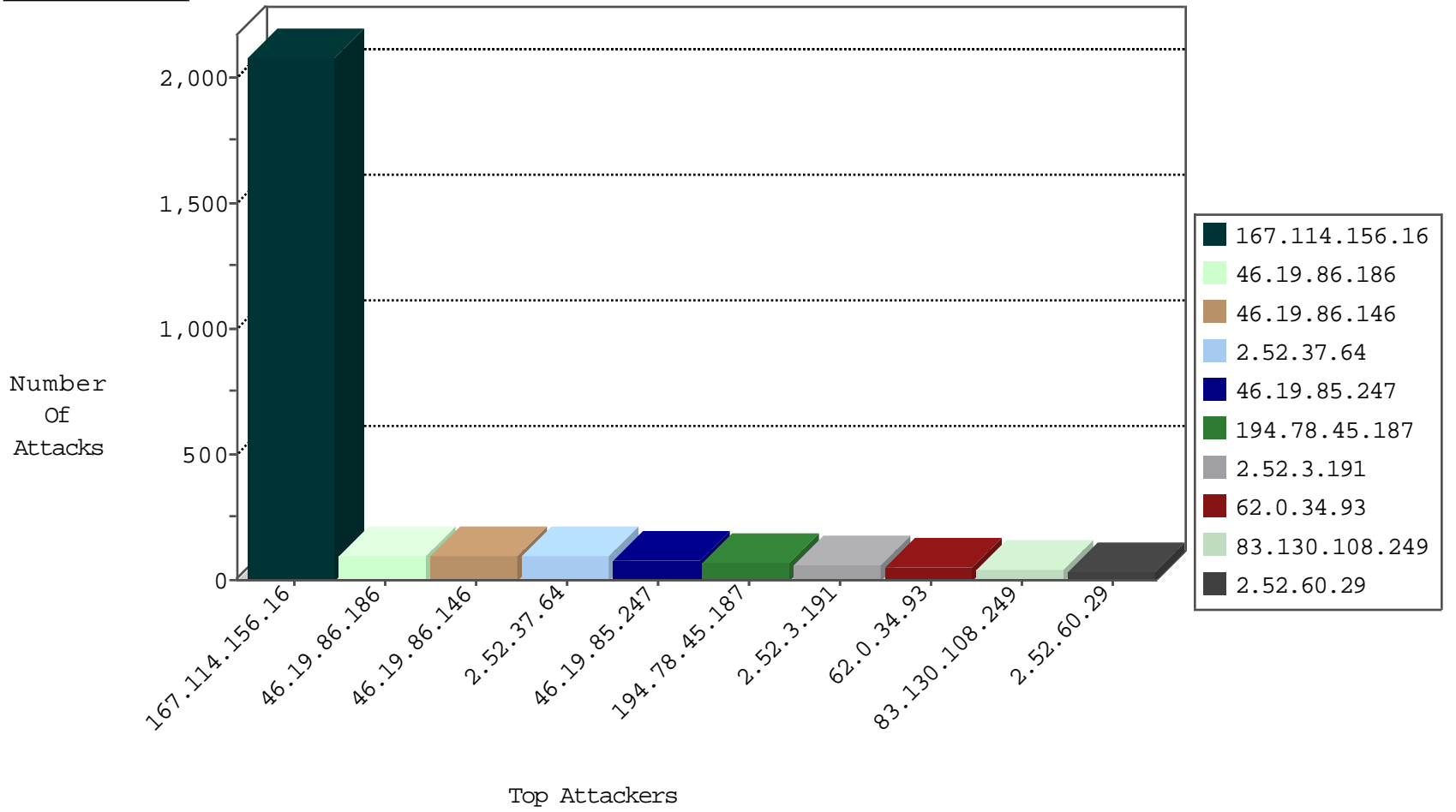
IDF Under Attack Daily Report



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	3062
2.52.37.64	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	10
31.13.160.217	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	6
107.150.60.246	United States	147.237.72.166	aka.idf.il	block-sp-trafl	drop	1
37.26.146.155	Israel	147.237.72.156	aman.idf.il	TCP handshake violation, first packet not syn	drop	1
63.141.227.98	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
107.150.55.212	United States	147.237.0.15	kosher-kravi.idf.i	block-sp-trafl	forward	1

01-13-2016-11:04:07 to 01-13-2016-12:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
193.201.227.7	147.237.76.198	Ukraine	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.231	147.237.8.45		e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.217.100	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.102.170.34	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
61.216.2.13	147.237.0.16	Taiwan	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.186.129	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
185.130.5.231	147.237.72.166		aka.idf.il	ET SCAN Potential SSH Scan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
91.135.102.187	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
2.54.212.3	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.78.45.187	Belgium	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	65
2.52.37.64	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	58
83.130.108.249	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	43
109.186.104.27	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
2.52.3.191	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	24
109.65.128.12	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
157.55.39.0	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
46.19.86.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.52.3.191	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
2.54.22.202	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.52.37.64	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
46.19.86.183	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
2.52.3.191	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
2.52.3.191	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
2.52.60.29	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
109.226.21.17	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
46.19.86.213	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
31.210.188.65	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.54.52.174	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.253.192.48	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
2.54.29.116	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.9	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
82.80.196.44	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
192.3.211.48	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
2.52.37.64	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.128	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.3.211.48	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
132.72.154.116	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.137.218	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.60.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
80.246.136.168	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.114.91.244	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.14.94	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.60.29	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	6
46.19.85.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.148.208	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.132.246.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.60.29	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.54.151.0	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
61.216.2.13	Taiwan	147.237.77.233	atal.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	6
109.253.137.218	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.52.60.29	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	drop	SAM rule	drop	6
46.19.85.9	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.173	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
2.54.18.236	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.203	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
46.19.86.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
46.19.85.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
62.0.34.93	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	46
46.19.85.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
46.19.86.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	23
46.19.86.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
46.19.85.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
109.253.147.109	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 109.253.147.109	Block	13
2.54.55.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
82.81.2.165	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	5
82.81.2.165	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 82.81.2.165	Block	4
17.138.57.83	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.57.83	Block	4
82.81.2.165	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	3
185.32.179.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
46.19.85.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.227	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/general.aspx	Block	3
5.29.178.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
2.54.29.116	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.108	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
141.105.68.30	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	2
109.186.189.174	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	2
46.19.86.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
91.246.218.50	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	2
46.19.85.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.116.253.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.50.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.146	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtStreet in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	2
2.54.52.174	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
188.143.232.14	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/article/article.in.aspx/templates/sendtofriend/sendtofriend.aspx	Block	2
62.219.21.55	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
91.231.193.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
188.143.232.14	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/shared/usercontrols/headerupper/	Block	2
201.172.57.75	Mexico	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
91.246.218.50	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
185.3.146.196	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.127.252.168	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.148.208	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.253.133.125	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.147.197	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	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
61.216.2.13	Taiwan	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method	Block	1
212.117.136.6	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/x'x'x'x'x'	Block	1
88.230.53.194	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
188.143.232.15	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
80.246.136.168	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
31.13.160.217	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.13.160.217	Block	1
66.249.79.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/miluum.	Block	1
201.172.57.75	Mexico	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1