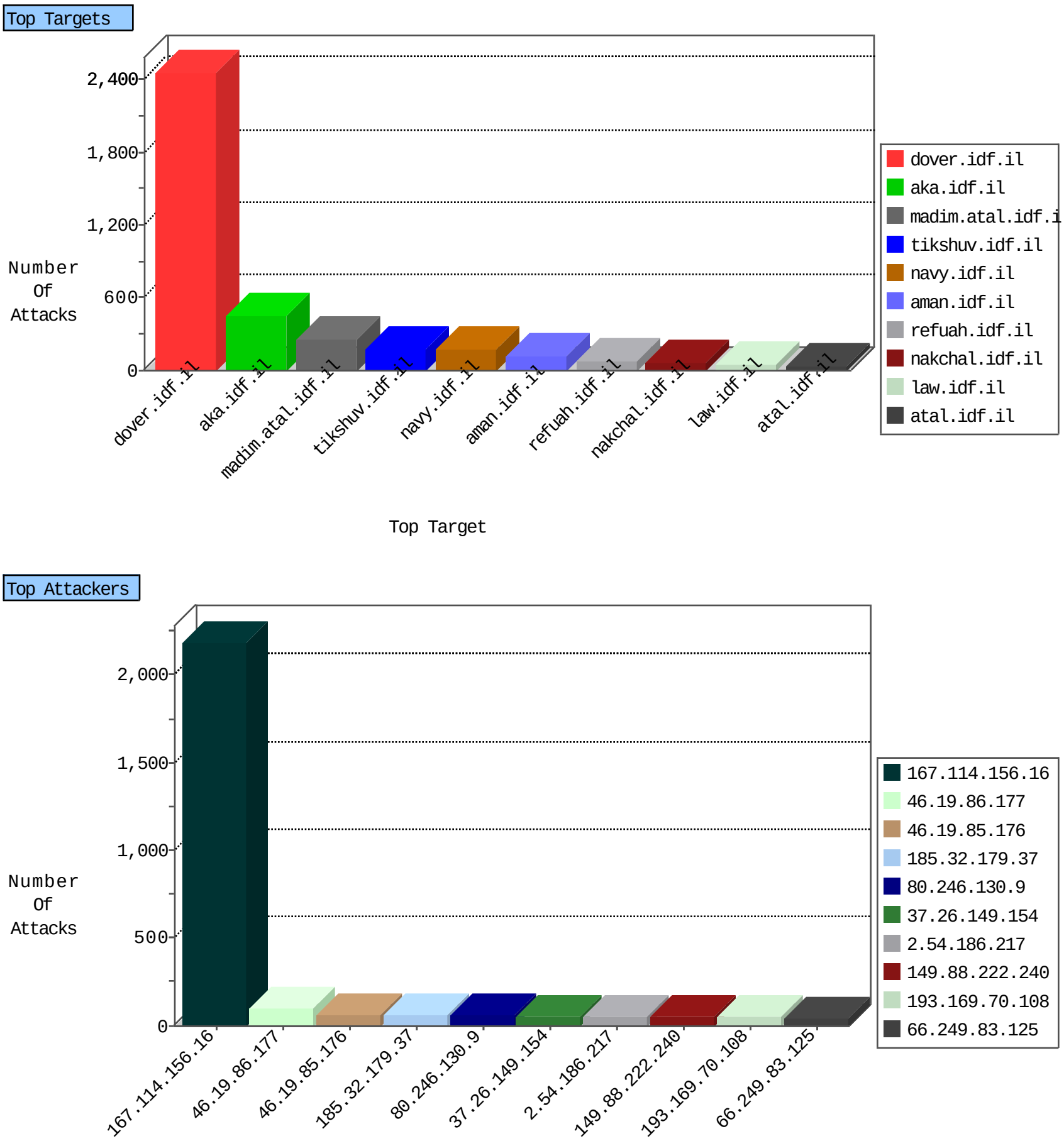
01-13-2016-16:04:05 to 01-13-2016-17:04:05

IDF Under Attack Daily Report



01-13-2016-16:04:05 to 01-13-2016-17:04:05

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	3212
37.26.149.154	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	22
82.145.219.99	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	11
46.19.86.107	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
109.253.132.185	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
31.168.133.226	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
107.150.55.213	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	1
185.130.5.224		147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
84.111.48.55	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
142.54.168.139	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	drop	1

01-13-2016-16:04:05 to 01-13-2016-17:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.186.21.169	Japan	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1

01-13-2016-16:04:05 to 01-13-2016-17:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.83.125	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	43
66.249.78.82	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
46.19.86.142	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.24.37.185	147.237.77.205	Bulgaria	prisha.idf.il	ET SCAN Potential SSH Scan	1
5.22.131.103	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.201.227.7	147.237.8.50	Ukraine	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.247	147.237.77.233		atal.idf.il	ET SCAN Potential SSH Scan	1
123.139.28.144	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
123.139.28.144	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
89.139.228.190	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.57.32.31	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
61.216.2.15	147.237.0.16	Taiwan	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
195.24.37.185	147.237.77.216	Bulgaria	dover.idf.il	ET SCAN Potential SSH Scan	1
45.32.36.233	147.237.76.38		e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
195.24.37.185	147.237.77.170	Bulgaria	maarachot.idf.il	ET SCAN Potential SSH Scan	1
192.118.11.120	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.247	147.237.76.38		e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
123.139.28.144	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
95.86.75.20	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.82.64.68	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
195.24.37.185	147.237.77.235	Bulgaria	sviva.idf.il	ET SCAN Potential SSH Scan	1

01-13-2016-16:04:05 to 01-13-2016-17:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.176	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	60
80.246.130.9	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	57
193.169.70.108	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	47
195.110.40.7	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
212.199.143.202	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
46.19.85.251	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
46.19.86.174	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
192.117.138.211	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
81.19.128.210	Russian Federation	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
37.26.149.154	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
37.26.149.154	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
37.26.149.154	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
192.117.138.210	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
141.105.68.30	Russian Federation	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
46.19.86.57	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.159	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
81.19.128.210	Russian Federation	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
2.52.183.245	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.86.132	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
185.32.179.127	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
188.120.148.176	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.175	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.210.212.229	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
84.111.226.239	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.94.15.222	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.231	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.183.136.112	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.222	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.160	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.94.15.222	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.231	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.44.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.136.112	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.29.167.48	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.222	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
149.78.252.118	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.160	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
65.51.48.134	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.168	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.175	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.160	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.220	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	5
46.19.85.175	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.220	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.175	Israel	147.237.76.86	navy.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
46.19.86.177	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	100
185.32.179.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	58
2.54.186.217	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	54
149.88.222.240	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	53
2.54.0.20	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
212.76.100.8	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	26
84.109.104.237	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	26
141.105.68.30	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 141.105.68.30	Block	19
138.134.192.10	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 138.134.192.10	Block	12
2.54.44.247	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 2.54.44.247	Block	11
81.218.70.243	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 81.218.70.243	Block	6
37.46.39.235	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	5
2.54.134.1	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
79.178.30.58	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for aka.idf.il/	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
176.13.13.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.116.96.38	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.116.96.38	Block	3
217.132.100.107	Israel	147.237.72.156	aman.idf.il	Distributed Malformed URL	Block	3
188.143.232.13	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.13	Block	3
79.180.172.72	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
217.132.100.107	Israel	147.237.72.156	aman.idf.il	Distributed Illegal HTTP Version	Block	2
217.132.100.107	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 217.132.100.107 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	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
84.94.38.200	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	2
217.132.100.107	Israel	147.237.72.156	aman.idf.il	Distributed Unknown HTTP Request Method	Block	2
188.143.232.41	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.41	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
95.86.99.181	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
79.178.30.58	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/	Block	2
37.26.147.180	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.66.132.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.117.138.210	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/defauly.aspx	Block	1
87.68.53.56	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
217.132.100.107	Israel	147.237.72.156	aman.idf.il	Multiple NULL Character in Header Name from 217.132.100.107	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1
46.19.86.249	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
173.208.136.170	United States	147.237.77.233	atal.idf.il	Admin Blocking	Block	1
2.54.4.15	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
81.218.185.236	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.82.64.68	Netherlands	147.237.76.86	navy.idf.il	Unauthorized URL Access to habbo.yt/public/css/960_12_col.css	Block	1
207.46.13.69	United States	147.237.0.34	tikshuv.idf.il	Suspicious Response Code	Block	1
46.19.85.10	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
138.134.192.10	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/2/size338x0/1802.jpg	Block	1
79.176.177.143	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
188.143.232.13	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/article.in.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
31.154.9.62	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	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
2.54.132.14	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
84.109.146.226	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
217.132.100.107	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Header Value from 217.132.100.107	Block	1