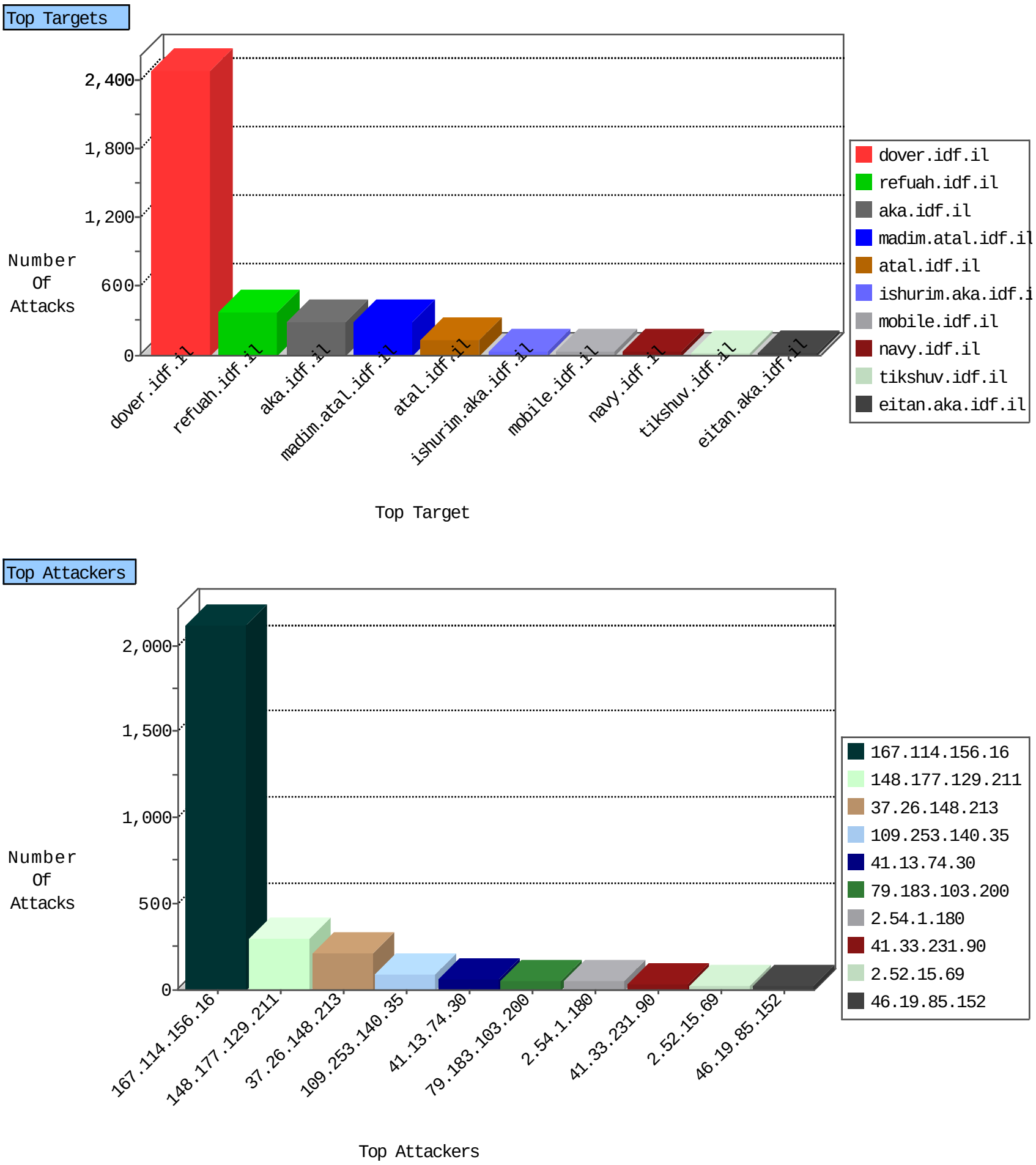
01-20-2016-11:04:06 to 01-20-2016-12:04:06

IDF Under Attack Daily Report



01-20-2016-11:04:06 to 01-20-2016-12:04:06

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	3168
212.199.112.144	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	109
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	12
84.228.177.238	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
84.111.225.26	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
149.78.154.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
148.177.129.211	Europe	147.237.76.42	refuah.idf.il	JLM_Purple_Con_Limit_Http	drop	3
148.177.129.211	Europe	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Http	drop	2
23.95.50.58	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
185.81.158.41		147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1

01-20-2016-11:04:06 to 01-20-2016-12:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.202.48.246	Germany	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	1
46.120.204.172	Israel	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	1
46.120.204.172	Israel	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

01-20-2016-11:04:06 to 01-20-2016-12:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2

01-20-2016-11:04:06 to 01-20-2016-12:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
148.177.129.211	Europe	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	183
109.253.140.35	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	90
41.13.74.30	South Africa	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	44
148.177.129.211	Europe	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	34
79.183.103.200	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
148.177.129.211	Europe	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	29
176.13.0.199	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
148.177.129.211	Europe	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	21
148.177.129.211	Europe	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid sequence number	monitor	21
41.239.25.227	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
172.56.5.130	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
41.13.74.30	South Africa	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
2.52.15.69	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
79.183.103.200	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
46.19.85.117	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	14
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
192.115.177.202	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
2.52.6.154	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
80.246.130.250	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
41.239.25.108	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
80.246.130.250	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
2.52.150.180	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
109.67.49.122	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
132.64.83.22	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
31.168.170.190	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
213.8.204.37	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
46.19.85.186	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
46.19.86.10	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.252	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.86.19	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.28	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.152	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.52.45.213	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.28	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.152	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.209.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
2.54.135.121	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.140.101	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.185.142	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
145.225.60.5	Germany	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	6
104.232.3.33		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.15.69	Israel	147.237.76.42	refuah.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
80.246.139.91	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
104.232.3.33		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
148.177.129.211	Europe	147.237.76.42	refuah.idf.il	Streaming Engine: TCP SYN Modified Retransmission	Data received before SYN was acknowledged. Stripping all packet data.	drop	5
2.54.145.93	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4

01-20-2016-11:04:06 to 01-20-2016-12:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.148.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	149
37.26.148.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	65
2.54.1.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
85.250.183.25	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	11
176.13.6.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
149.88.48.164	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 149.88.48.164	Block	4
37.26.148.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
176.13.8.96	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	4
2.54.50.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.196.4	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	3
2.54.176.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.188.208	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	3
176.13.2.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
52.33.66.29	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 52.33.66.29	Block	2
109.253.196.145	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	2
212.179.28.215	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
46.19.85.185	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
149.88.48.164	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	2
46.19.86.13	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.173.70	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/www.tikshuv.idf.il	Block	2
2.52.183.198	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
141.212.122.177	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
52.33.66.29	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
212.179.28.215	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
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
46.19.86.34	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.168.11.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
79.183.103.200	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
62.219.63.202	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
213.8.204.58	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
150.70.173.6	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.19.86.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.55	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/vb/sendmessage.php	Block	1
85.130.219.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.149.162	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
184.72.218.195	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/old/wp-admin/	Block	1
158.199.136.10	Japan	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1397-en/dover.aspx	Block	1
147.236.138.210	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
212.179.166.76	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
46.19.86.54	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
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	1
109.64.134.119	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 109.64.134.119	Block	1
37.26.147.205	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.21	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
213.151.32.163	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1

01-20-2016-11:04:06 to 01-20-2016-12:04:06