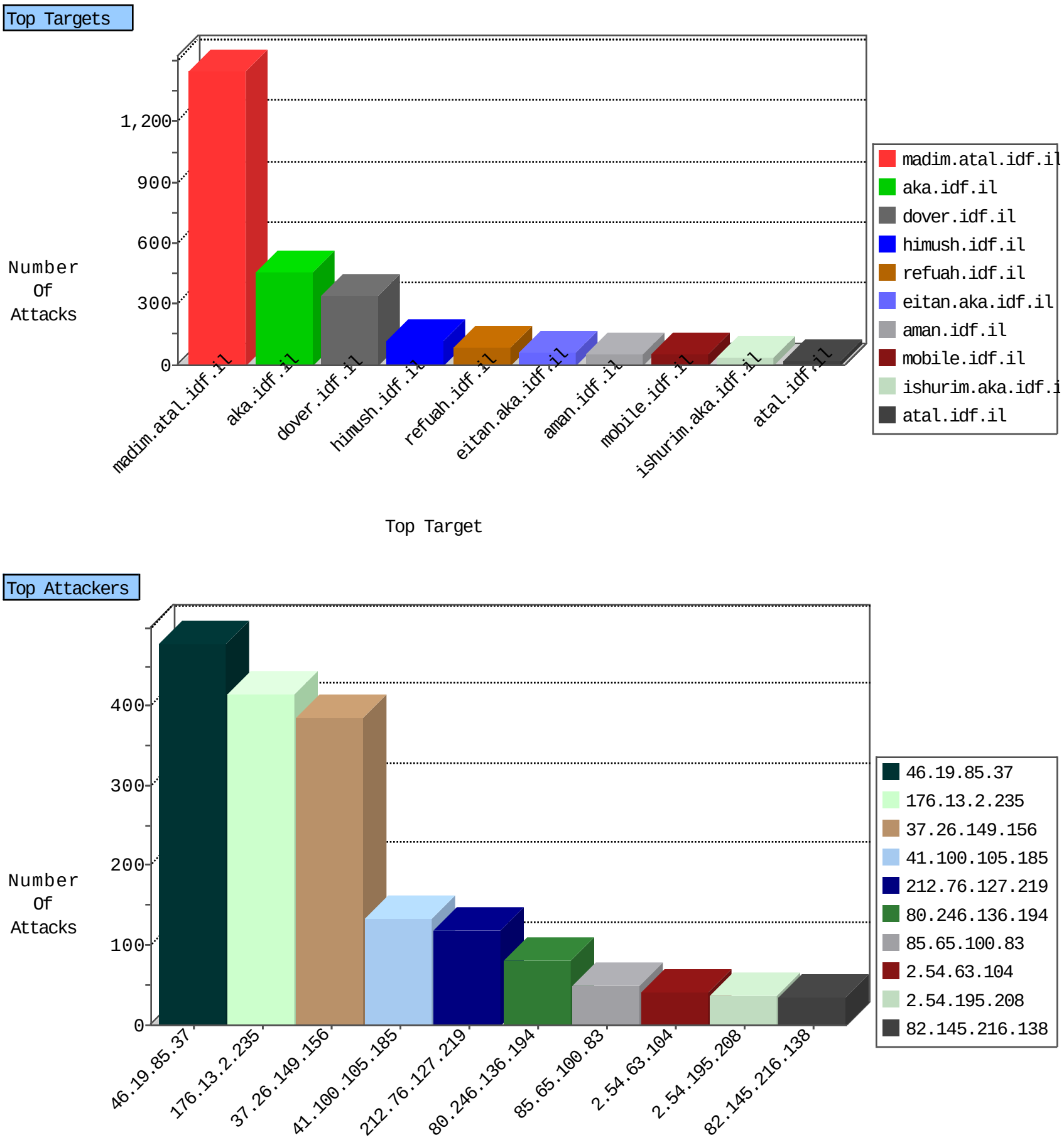
02-09-2016-16:04:07 to 02-09-2016-17:04:07

IDF Under Attack Daily Report



02-09-2016-16:04:07 to 02-09-2016-17:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.199.112.144	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	241
82.166.137.19	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	157
81.218.241.25	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	98
66.249.93.182	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
85.105.141.155	Turkey	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
71.6.216.36	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.201		147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1

02-09-2016-16:04:07 to 02-09-2016-17:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.100.105.185	Algeria	147.237.77.216	dover.idf.il	C091: HTTP: Access to - admin.asp	Block	1
95.8.21.149	Turkey	147.237.77.216	dover.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1

02-09-2016-16:04:07 to 02-09-2016-17:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
95.86.78.254	147.237.76.86	Israel	navy.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
41.100.105.185	147.237.77.216	Algeria	dover.idf.il	SERVER-WEBAPP admin.php access	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
41.100.105.185	147.237.77.216	Algeria	dover.idf.il	SERVER-WEBAPP login.htm access	1

02-09-2016-16:04:07 to 02-09-2016-17:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
85.65.100.83	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	50
82.145.216.138	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	35
207.241.229.103	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
176.13.9.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
41.100.105.185	Algeria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
46.19.85.65	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
46.19.86.250	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
85.64.77.194	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
192.116.218.93	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
79.182.22.75	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
46.19.85.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.149.216	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.154.177	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.46.38.31	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.85.65	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
185.120.126.29		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.64.166.48	Israel	147.237.77.170	maarachot.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
5.102.195.199	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
5.102.254.189	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.149.148	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.40	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.76.127.219	Israel	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
5.102.221.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.207	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.178.127.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.53.96	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.182.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.148	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.179.174.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.207	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.200.205.2	Israel	147.237.72.166	aka.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
159.220.75.7	United Kingdom	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
37.26.149.148	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
109.253.208.163	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.104.168.50	United Kingdom	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
2.52.166.11	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
31.210.186.78	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
81.218.241.25	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	6
212.76.127.10	Israel	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
93.158.152.201	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
146.200.236.142	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
77.127.253.121	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.149	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.40	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
80.246.137.190	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4

02-09-2016-16:04:07 to 02-09-2016-17:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	283
176.13.2.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	202
46.19.85.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	195
37.26.149.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	176
37.26.149.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	170
176.13.2.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	122
212.76.127.219	Israel	147.237.76.30	himush.idf.il	Distributed Too Many of the Same Response Code (404)	Block	112
176.13.2.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	91
80.246.136.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	79
41.100.105.185	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.100.105.185	Block	53
2.54.63.104	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	42
37.26.149.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	41
2.54.195.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
41.100.105.185	Algeria	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	33
41.100.105.185	Algeria	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	16
95.35.10.73	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 95.35.10.73	Block	15
79.182.22.75	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	4
176.13.2.72	Israel	147.237.76.42	refuah.idf.il	Distributed Parameter Type Violation on www.refua.atal.idf.il/1518-he/refuah.aspx parameter ctl00$ContentPlaceHolder1$txtLastName	Block	4
95.8.21.149	Turkey	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.8.21.149	Block	4
95.8.21.149	Turkey	147.237.77.216	dover.idf.il	PHP Attempt	Block	3
46.116.114.22	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/g/yus	Block	3
85.254.78.159	Latvia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
46.19.85.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
85.254.78.159	Latvia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	3
46.19.86.185	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.250	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.216	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
144.173.23.95	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/resources/ppt/yohalan_eng.ppt.	Block	2
2.54.54.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
95.8.21.149	Turkey	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 95.8.21.149	Block	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	2
82.80.69.90	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1216-he/miluim.aspx	Block	2
66.249.66.26	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-9070-he/atal.aspx	Block	1
128.232.110.28	United Kingdom	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
84.94.40.215	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/guyus	Block	1
194.90.116.67	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$80 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
173.199.202.163	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/4/myball.cur	Block	1
79.116.26.74	Romania	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 79.116.26.74	Block	1
109.67.81.85	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 109.67.81.85 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
62.0.103.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
217.132.37.88	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$41 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
93.172.251.17	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	1
176.13.5.88	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
79.182.112.246	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
67.87.166.176	United States	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
2.52.156.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
95.8.21.149	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
46.116.162.16	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
194.90.116.67	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
5.22.134.204	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1

02-09-2016-16:04:07 to 02-09-2016-17:04:07