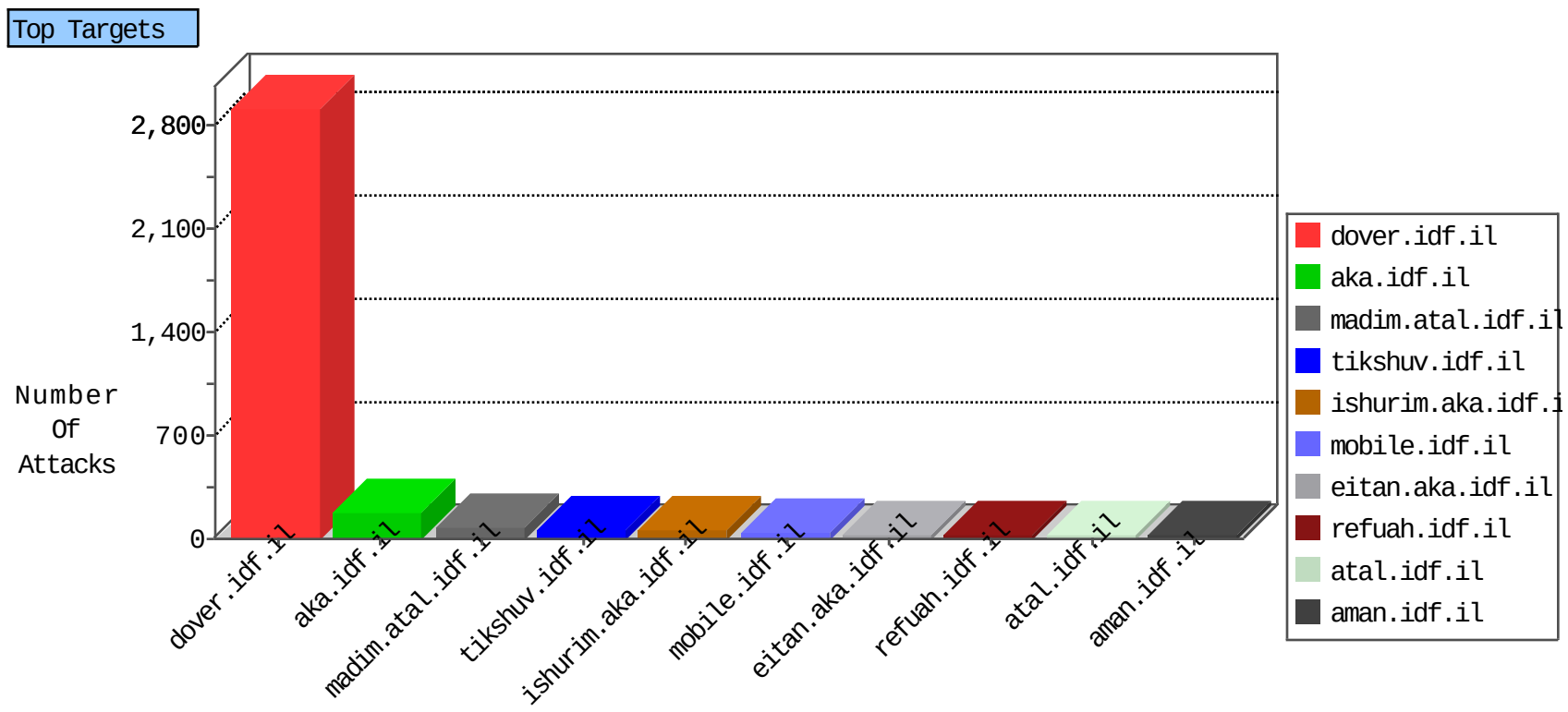
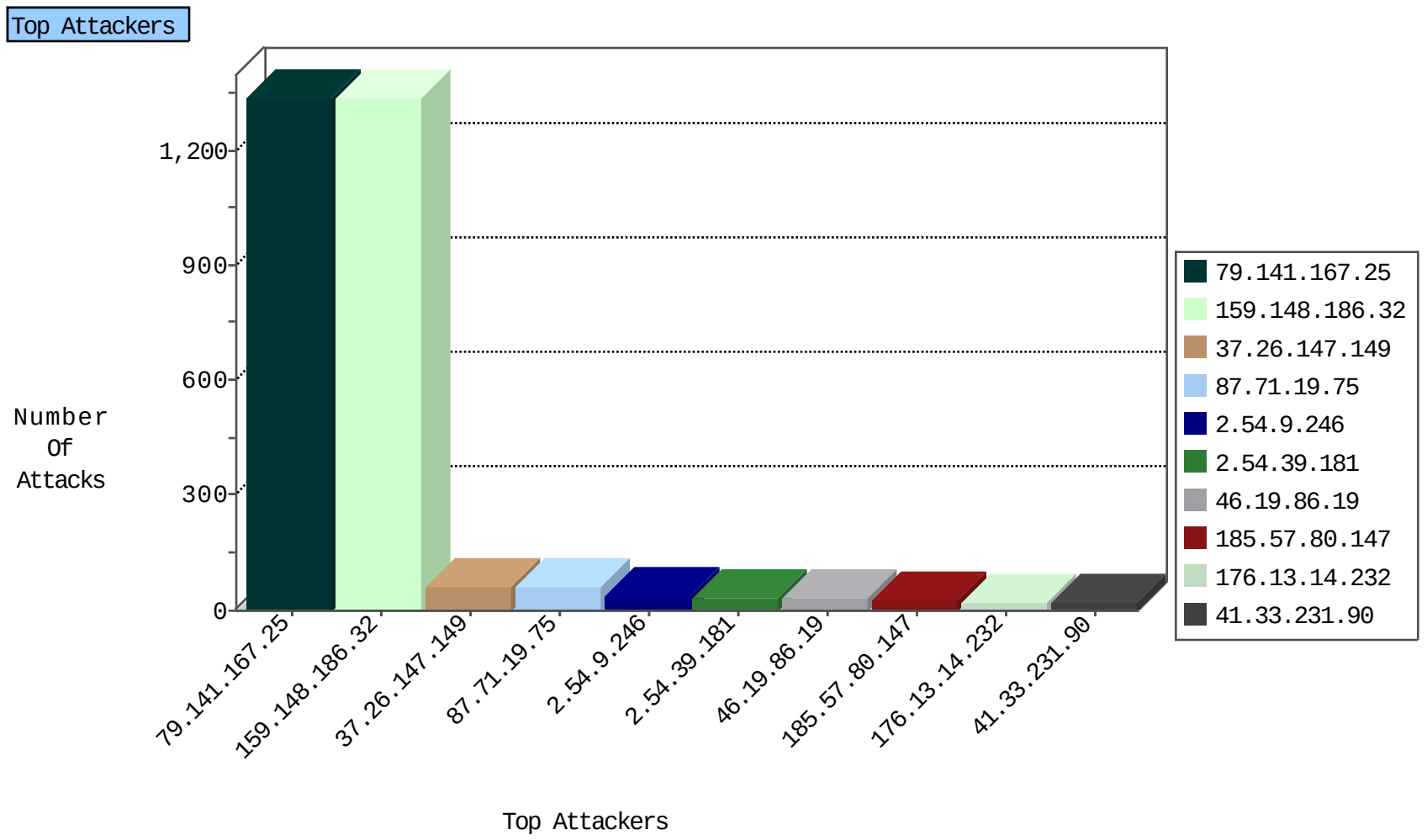
02-17-2016-15:04:09 to 02-17-2016-16:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-17-2016-15:04:09 to 02-17-2016-16:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.141.167.25	Switzerland	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-cat	dest-reset	1210
31.168.240.21	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
109.64.162.209	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
147.236.238.250	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
185.130.5.224		147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
104.238.129.180		147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
54.210.110.87	United States	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1
185.130.5.224		147.237.76.148	gqcenter.aka.idf.il	Block_Udp_All_Nets	drop	1
104.238.129.180		147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.224		147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
104.238.129.180		147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
85.64.117.52	Israel	147.237.76.86	navy.idf.il	Anomaly-TCP-shortheader	dest-reset	1
104.243.223.8		147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

02-17-2016-15:04:09 to 02-17-2016-16:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-17-2016-15:04:09 to 02-17-2016-16:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.141.167.25	147.237.77.216	Switzerland	dover.idf.il	ET CURRENT_EVENTS Inbound Low Orbit Ion Cannon LOIC DDOS Tool desu string	4
64.233.172.211	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.15.144	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
46.120.66.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.189.34	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
190.216.146.151	147.237.0.15	Chile	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
89.139.155.49	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-17-2016-15:04:09 to 02-17-2016-16:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.141.167.25	Switzerland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	98
2.54.39.181	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
46.19.86.19	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
185.57.80.147	Romania	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
79.141.167.25	Switzerland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
149.78.3.164	Israel	147.237.77.216	dover.idf.il	HTTP Format Sizes	'User-Agent' header length exceeded maximum allowed length	monitor	14
46.19.86.198	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.141.167.25	Switzerland	147.237.77.216	dover.idf.il	SYN Attack		reject	12
109.67.213.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.116.232.69	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
46.19.85.74	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
2.54.9.246	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
2.54.9.246	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
2.54.9.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.54.9.246	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
2.52.35.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.116.239.196	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
79.181.61.163	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
109.253.134.109	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
212.117.136.6	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
217.132.0.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.219.133.130	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.21.194	Israel	147.237.77.212	e.dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
2.54.13.77	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.81.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
132.72.129.240	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.139	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.253.134.109	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.210.186.123	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.191	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
37.26.148.133	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
84.108.22.169	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
91.221.59.22	Germany	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
176.12.135.223	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
91.221.59.22	Germany	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
176.13.16.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.54.141.122	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
2.54.18.171	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.186.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.129	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.176.188.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.118.12.102	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
84.228.200.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.57.80.147	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
82.81.57.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-17-2016-15:04:09 to 02-17-2016-16:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
159.148.186.32	Latvia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 159.148.186.32	Block	1331
37.26.147.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	60
87.71.19.75	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	59
176.13.14.232	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	23
109.253.140.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
37.26.148.133	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
46.19.85.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.32.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.151	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	2
159.148.186.32	Latvia	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1129-he/dover.aspx	Block	2
46.19.86.239	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
62.0.102.190	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
109.253.217.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
93.172.60.195	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
207.46.13.181	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.86.198	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
146.185.234.48	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
79.181.217.210	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl99 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
2.54.21.0	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
213.151.35.216	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$22 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	1
54.147.176.220	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18485-he/dover.aspx	Block	1
41.68.197.251	Egypt	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
5.29.123.175	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
212.179.21.194	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.69.58	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
188.120.130.73	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
157.55.39.32	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/901-10737-en/cogat.aspx 	Block	1
84.111.62.101	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$1 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
2.54.134.225	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
213.151.59.35	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/1181-he/idfg.aspx&sa=u&ved=0ahukewj9zjjg8f7kahwlphqkhbijb04qfggnmai&usg=afqjcnekk0veko_xpraf7ctxhekj6c3m7q	Block	1
193.33.2.113	Spain	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
159.148.186.32	Latvia	147.237.77.216	dover.idf.il	SQL injection on parameter ctl00$ContentPlaceHolder1$txtPhone in www.idf.il/1038-ar/dover.aspx	Block	1
41.68.197.251	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
5.29.249.7	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 5.29.249.7 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
79.177.108.204	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
212.199.57.200	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.121.109.190	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 46.121.109.190	Block	1
188.120.130.73	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 188.120.130.73	Block	1
157.55.39.208	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
2.54.178.155	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$81 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
216.55.112.119	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/spanish/	Block	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
62.219.129.25	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
159.148.186.32	Latvia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1008-ar/3590757893399431968.aspx	Block	1
5.29.249.7	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
132.72.129.240	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
79.178.134.195	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$96 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
213.57.139.187	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed PHP Attempt	Block	1
46.121.109.190	Israel	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	1

02-17-2016-15:04:09 to 02-17-2016-16:04:09