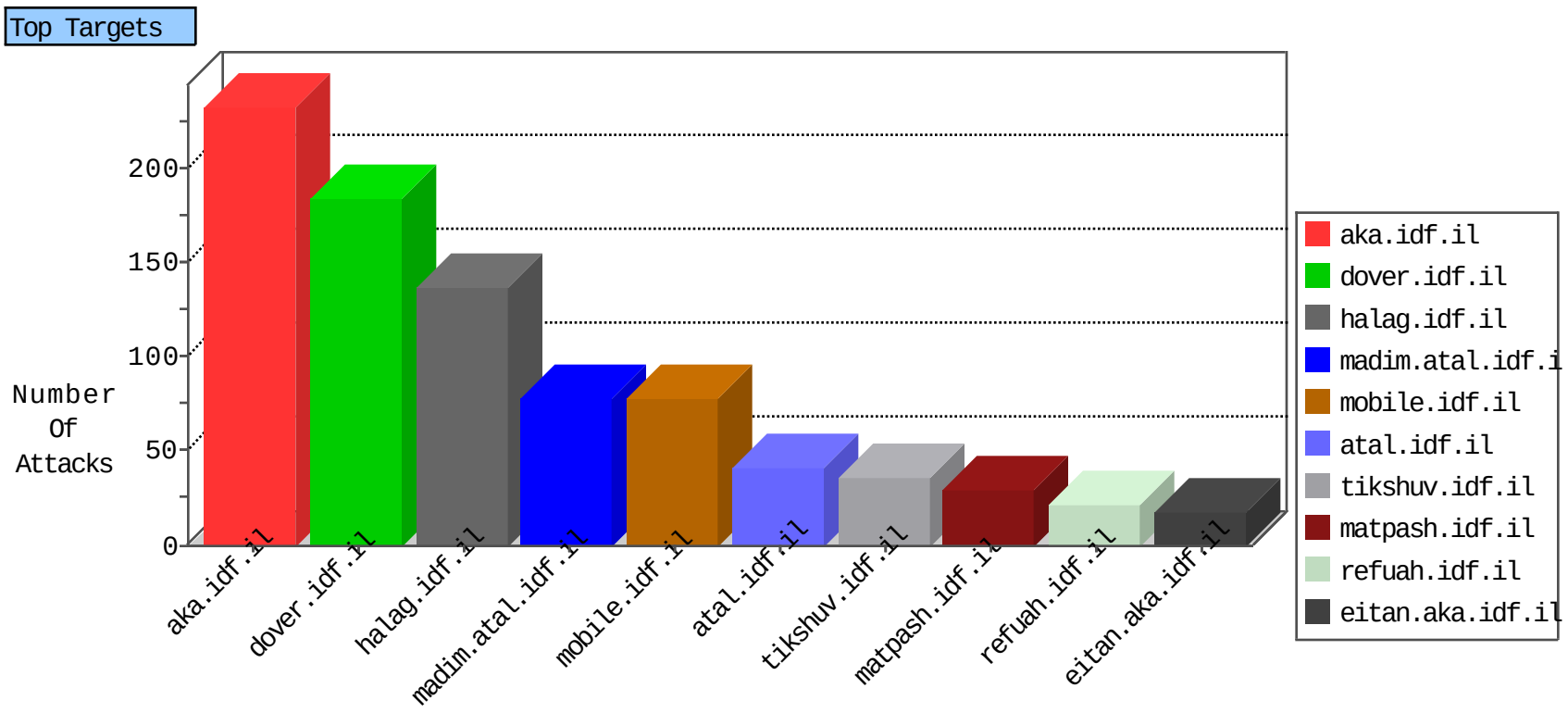
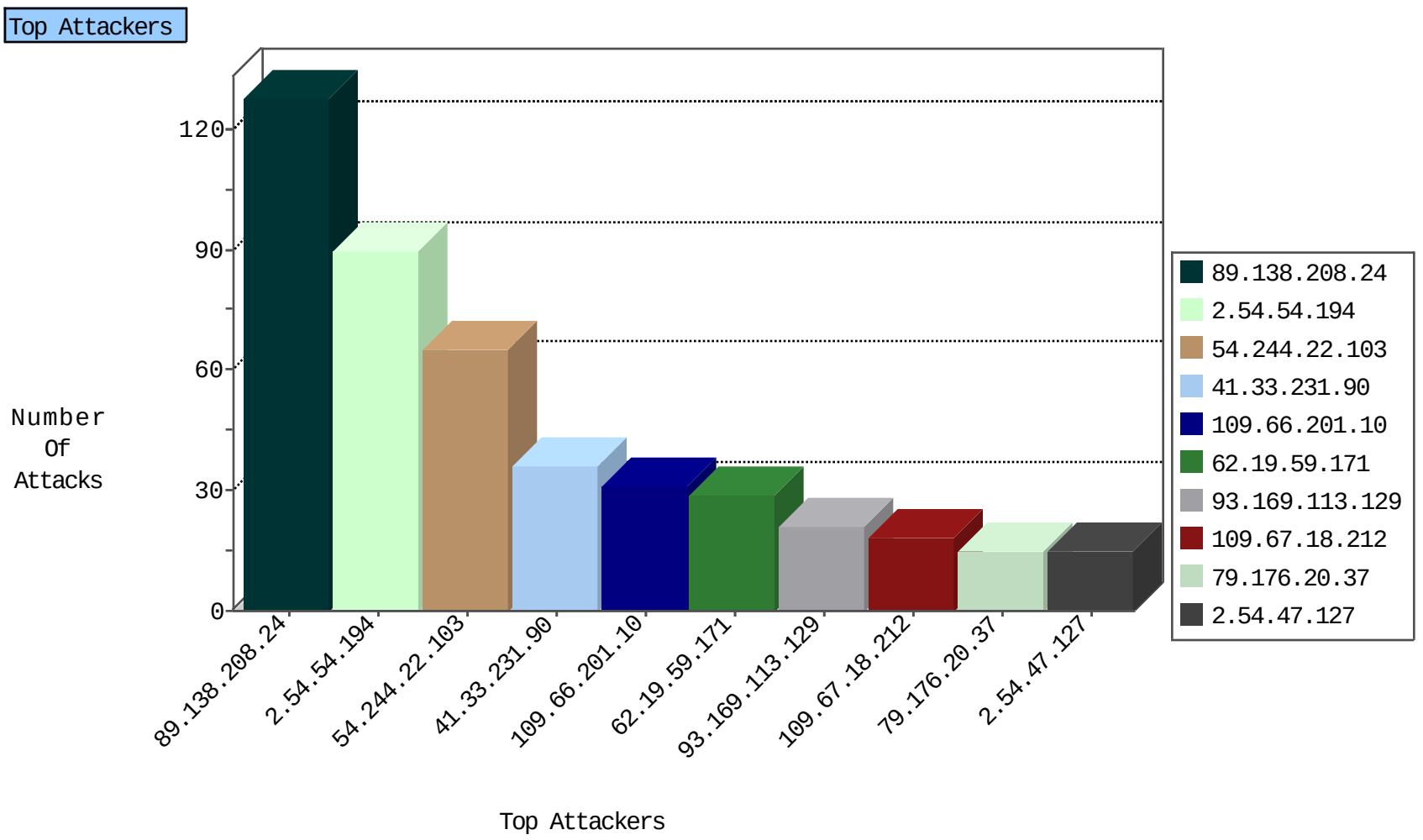
02-06-2016-15:04:02 to 02-06-2016-16:04:02

IDF Under Attack Daily Report





02-06-2016-15:04:02 to 02-06-2016-16:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
157.55.39.209	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
182.52.206.206	Thailand	147.237.77.212	e.dover.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
185.130.5.174		147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
199.48.164.223	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1

02-06-2016-15:04:02 to 02-06-2016-16:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-06-2016-15:04:02 to 02-06-2016-16:04:02

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	4
183.61.109.189	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 1024	1
125.212.232.144	147.237.77.170	Vietnam	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
93.189.26.18	147.237.76.38	Austria	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
79.177.35.199	147.237.76.30	Israel	himush.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
201.48.50.33	147.237.72.14	Brazil	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
201.48.50.33	147.237.0.33	Brazil	idf.il	ET SCAN Potential SSH Scan	1
190.124.35.115	147.237.0.16	Nicaragua	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
183.61.109.189	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 3072	1
125.212.232.144	147.237.77.170	Vietnam	maarachot.idf.il	ET SCAN NMAP -sS window 3072	1
125.212.232.144	147.237.77.170	Vietnam	maarachot.idf.il	ET SCAN NMAP -f -sS	1
91.201.236.114	147.237.77.121	Ukraine	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
201.48.50.33	147.237.72.166	Brazil	aka.idf.il	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1
201.48.50.33	147.237.0.35	Brazil	akaws.idf.il	ET SCAN Potential SSH Scan	1
50.18.225.195	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER PyCurl Suspicious User Agent Inbound	1
201.48.50.33	147.237.0.19	Brazil	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
190.124.35.115	147.237.0.16	Nicaragua	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
187.38.150.123	147.237.77.216	Brazil	dover.idf.il	ET SCAN Potential SSH Scan	1

02-06-2016-15:04:02 to 02-06-2016-16:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
89.138.208.24	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	127
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
2.54.54.194	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	36
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	32
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	27
62.19.59.171	Italy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
2.54.54.194	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
2.54.54.194	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	18
109.67.18.212	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
2.54.54.194	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
79.176.20.37	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
77.126.220.173	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.47.127	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
208.115.113.84	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	11
37.26.149.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
93.169.113.129	Romania	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
93.169.113.129	Romania	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
64.19.78.243	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
109.65.120.238	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.213.80.144	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
62.19.59.171	Italy	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.213.80.144	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.176.209.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.31	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
66.249.78.230	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.148.203	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	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
84.109.18.52	Israel	147.237.77.243	mobile.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
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.15	Israel	147.237.77.233	atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.136.47	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
49.201.251.206	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
94.230.86.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.108.17.49	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
84.228.114.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.131.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.67.106.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.126.72		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.32	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.31.117	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.135.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.166.100.40	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.20.224	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.28.167.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.33.231	Israel	147.237.0.19	madim.atal.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.85.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-06-2016-15:04:02 to 02-06-2016-16:04:02

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
46.19.86.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-06-2016-15:04:02 to 02-06-2016-16:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.66.201.10	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	31
2.54.168.5	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
2.52.31.117	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
186.202.153.185	Brazil	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 186.202.153.185	Block	5
46.19.85.216	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
2.54.55.25	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
149.78.179.198	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	3
185.32.179.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
149.78.254.79	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	3
87.69.92.46	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
216.104.160.77	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 216.104.160.77	Block	3
109.253.212.167	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.54.47.127	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.134	Block	3
149.78.179.198	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 149.78.179.198	Block	2
46.28.66.2	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.28.66.2	Block	2
85.65.202.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.82	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
77.126.220.173	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
46.19.86.31	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
84.228.97.201	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.177.121.26	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17454-en/kkkkkkk=d069718ekkkkkkk_d069718e	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
89.138.208.24	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
37.237.205.20	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
2.52.31.117	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	1
84.108.139.229	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
77.125.87.141	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 77.125.87.141	Block	1
79.178.102.56	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$76 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
66.249.78.230	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.65.109.34	Israel	147.237.77.216	dover.idf.il	Extremely Long Parameter in www.idf.il %D8%B3%D8%A3%D9%86%D8%AA%D9%82%D9%85+%D9%85%D9%86+%D8%AF%D8%AE%D9%88%D9%84+%D8%A7%D9%84%D9%85%D8%B3%	Block	1
46.19.85.15	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
2.52.33.231	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
84.109.18.52	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
209.159.138.19	United States	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
77.125.87.141	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/	Block	1
46.28.66.2	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/homepage.aspx/templates/social/twitter.aspx	Block	1
5.101.217.107	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1283-en/dover.aspx	Block	1
79.179.103.186	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
66.249.79.45	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/2/109622.pdf	Block	1
2.52.188.87	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
84.111.233.43	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.148.31.88	Lithuania	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1283-en/dover.aspx parameter ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker	Block	1
157.55.39.208	United States	147.237.77.216	dover.idf.il	Abnormally Long Request URL	Block	1
87.69.92.46	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in www.atal.idf.il/1437-he/atal.aspx	Block	1
5.101.217.118	Russian Federation	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1283-en/dover.aspx parameter ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker	Block	1
79.183.32.200	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	1

02-06-2016-15:04:02 to 02-06-2016-16:04:02