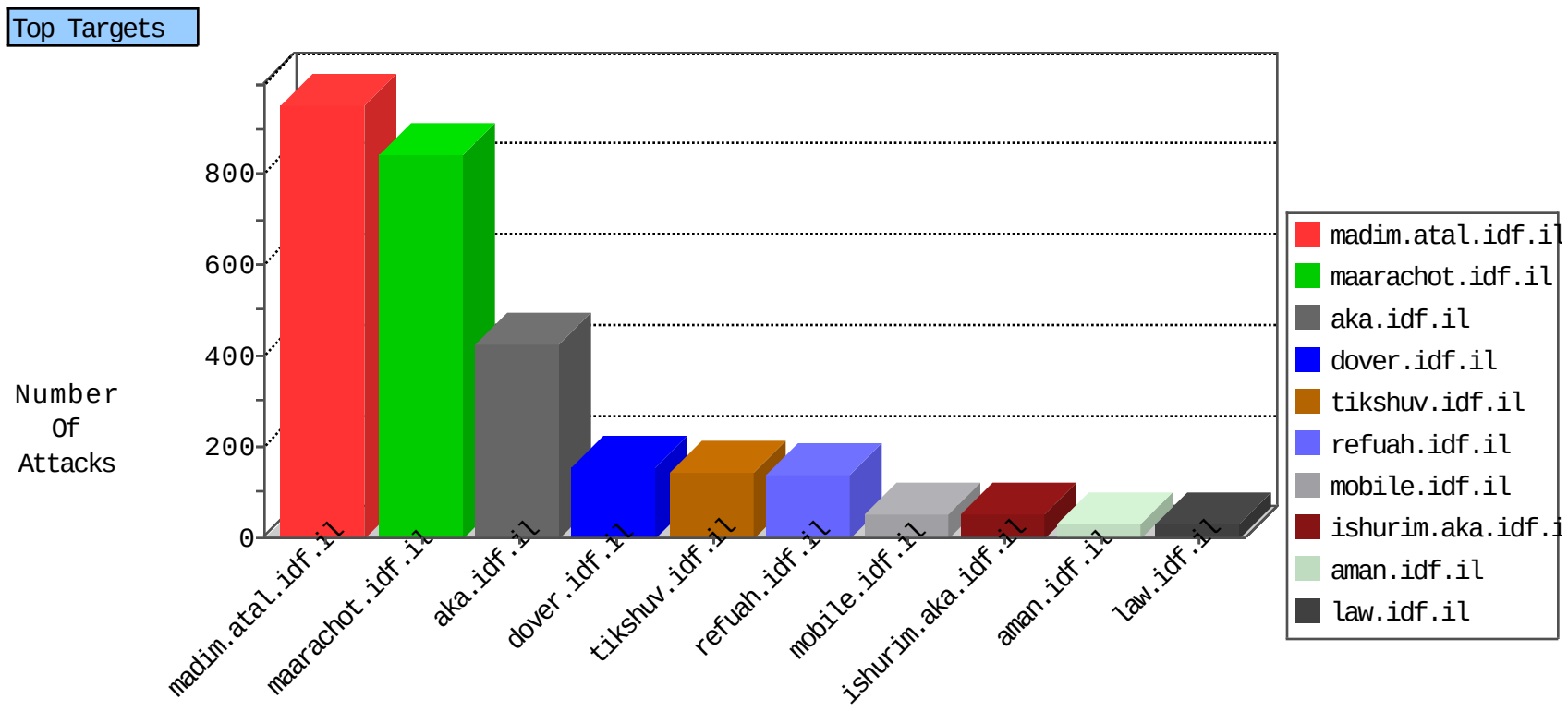
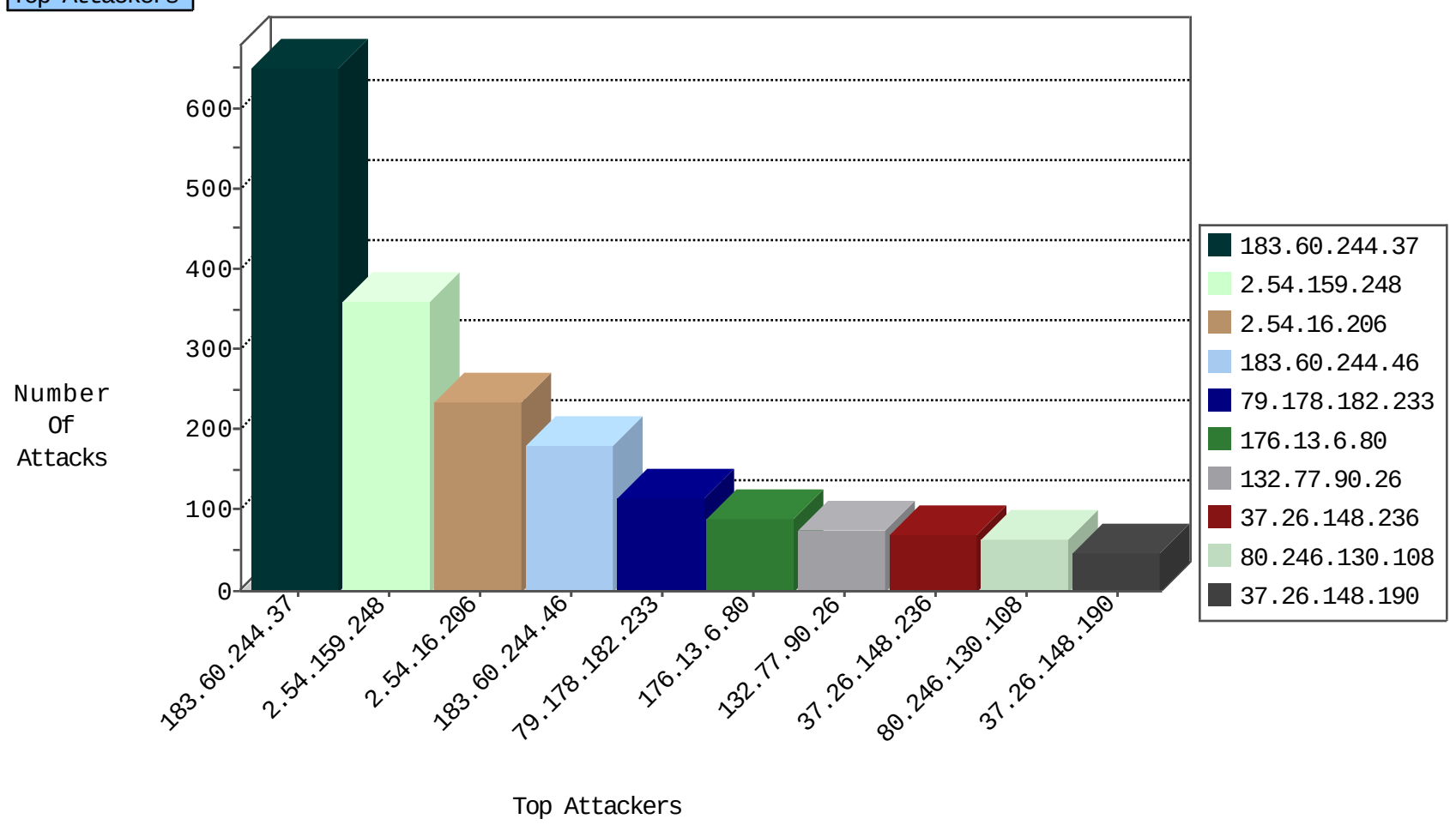
02-08-2016-15:04:06 to 02-08-2016-16:04:06

IDF Under Attack
Daily Report

Top Targets



Top Attackers



02-08-2016-15:04:06 to 02-08-2016-16:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.8.57.201	Israel	147.237.72.166	aka.idf.il	HTTP-POST-Segmented-DoS	dest-reset	619
109.64.130.186	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	16
198.58.102.156	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
0.0.0.0		147.237.72.166	aka.idf.il	HTTP-POST-Segmented-DoS	dest-reset	4
81.218.56.245	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
31.168.133.226	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
81.218.56.125	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
159.122.252.41	Netherlands	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
159.122.252.41	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
85.25.43.94	Germany	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

02-08-2016-15:04:06 to 02-08-2016-16:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
183.60.244.37	China	147.237.77.170	maarachot.idf.il	C003: HTTP: phpMyAdmin access	Block	4
183.60.244.46	China	147.237.77.170	maarachot.idf.il	C003: HTTP: phpMyAdmin access	Block	1
109.90.211.122	Germany	147.237.77.216	dover.idf.il	C106: HTTP: majestic bot	Block	1

02-08-2016-15:04:06 to 02-08-2016-16:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
132.72.138.1	147.237.72.167	Israel	ishurim.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	5
79.180.162.55	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
179.43.141.234	147.237.77.61	Switzerland	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
79.176.212.1	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
114.112.90.54	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 1024	1
68.180.229.239	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.141.99	147.237.72.166	Israel	aka.idf.il	GPL SCAN myscan	1
46.19.85.128	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.34.171	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
198.20.69.74	147.237.77.243	United States	mobile.idf.il	ET DROP Dshield Block Listed Source	1
2.54.137.153	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.69.172.152	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.62.18.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.20.168	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.94.18.213	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.77.19	Sweden	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.8.50	Sweden	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
80.178.204.49	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.0.15	China	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
79.178.164.104	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.100.218	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.141.99	147.237.72.166	Israel	aka.idf.il	INDICATOR-SCAN myscan	1
54.67.38.74	147.237.77.233	United States	atal.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
109.160.242.253	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.8.57.201	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
31.210.188.27	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.140.163	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.200.205.71	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.52.49.57	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.250.185.188	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
82.117.208.243	147.237.77.212		e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
193.105.134.220	147.237.76.31	Sweden	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
81.218.251.250	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.60.244.37	147.237.77.170	China	maarachot.idf.il	GPL WEB_SERVER WEB-MISC JBoss web-console access	1

02-08-2016-15:04:06 to 02-08-2016-16:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
132.77.90.26	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	75
37.26.148.236	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	70
46.19.85.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
109.253.139.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
188.32.231.27	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	14
82.166.29.153	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.148.177	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
82.80.180.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.20	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.116.205.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.181.222.64	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
62.0.207.1	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.156	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
109.253.143.209	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.32	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
77.37.222.199	Russian Federation	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.170	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.12.105	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
37.26.148.178	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.28.186.183	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.131.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.156	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.156	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.188.40.6	Russian Federation	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
79.182.188.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.130.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.187.65	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.0.200.202	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
37.26.147.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.187.109	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.109.80.223	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
37.26.146.223	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
46.19.85.13	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
87.70.2.180	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
82.166.198.189	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
87.71.2.106	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
37.26.146.223	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	5
95.108.168.68	Russian Federation	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
5.162.249.202	Oman	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
207.46.13.1	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
2.54.159.248	Israel	147.237.0.19	madim.atal.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.52.49.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
80.246.139.38	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
189.219.49.81	Mexico	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
5.29.203.106	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
189.219.49.81	Mexico	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
67.212.188.11	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
189.219.49.81	Mexico	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
109.253.143.209	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	4

02-08-2016-15:04:06 to 02-08-2016-16:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
183.60.244.37	China	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 183.60.244.37	Block	517
2.54.159.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	192
2.54.159.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	164
183.60.244.46	China	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 183.60.244.46	Block	141
2.54.16.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
2.54.16.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	102
176.13.6.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
79.178.182.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	80
183.60.244.37	China	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	67
80.246.130.108	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	65
183.60.244.37	China	147.237.77.170	maarachot.idf.il	Multiple Admin Blocking from 183.60.244.37	Block	60
37.26.148.190	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
77.126.168.65	Israel	147.237.72.167	ishurim.aka.idf.i	Too Many of the Same Response Code (404) in Session from 77.126.168.65	Block	35
79.178.182.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	32
46.19.86.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
2.54.16.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	24
183.60.244.46	China	147.237.77.170	maarachot.idf.il	Distributed Admin Blocking	Block	21
80.246.136.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
46.19.86.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
183.60.244.46	China	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	18
2.54.182.152	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	15
46.19.86.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
46.19.86.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
37.26.148.177	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
176.13.6.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	5
79.178.182.233	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	4
192.118.10.10	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.118.10.10	Block	4
192.116.94.110	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/163-he/patzar.aspx	Block	3
46.19.86.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
188.143.232.10	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1283-en/dover.aspx	Block	3
109.253.215.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
188.143.232.11	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$datepicker	Block	3
176.13.16.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.20.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
93.172.3.227	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
37.26.148.201	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
5.29.242.96	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	2
149.88.234.40	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$18 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
109.253.133.44	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
213.8.204.11	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 213.8.204.11	Block	2
199.203.123.201	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/964-he/patzar.aspx	Block	2
176.13.6.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Parameter Type Violation on madim.atal.idf.il/mobile/1088-he/meretz.aspx parameter ctl00$ContentPlaceHolder1$txtStreet	Block	1
104.131.161.55	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
37.26.148.190	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtStreet in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Illegal Byte Code Character in Method Ã„hÂ„Ã•;Â–{*Ã'[[#8]]Â«Â‰tÃ?Â™'Â¿i+[[#11]]Â¹bÃ¢hÃŒ+ÃªÂ™Ã¾Ã¼[[#2]]Â®Â¢ClÃ†v2ÂŠ<~Â?[[#17]]EuÂ¤WLÃ„)Â–]#65Ã·Ã?	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
183.60.244.46	China	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/issmall	Block	1
5.29.242.96	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 5.29.242.96	Block	1
147.236.34.110	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1

02-08-2016-15:04:06 to 02-08-2016-16:04:06