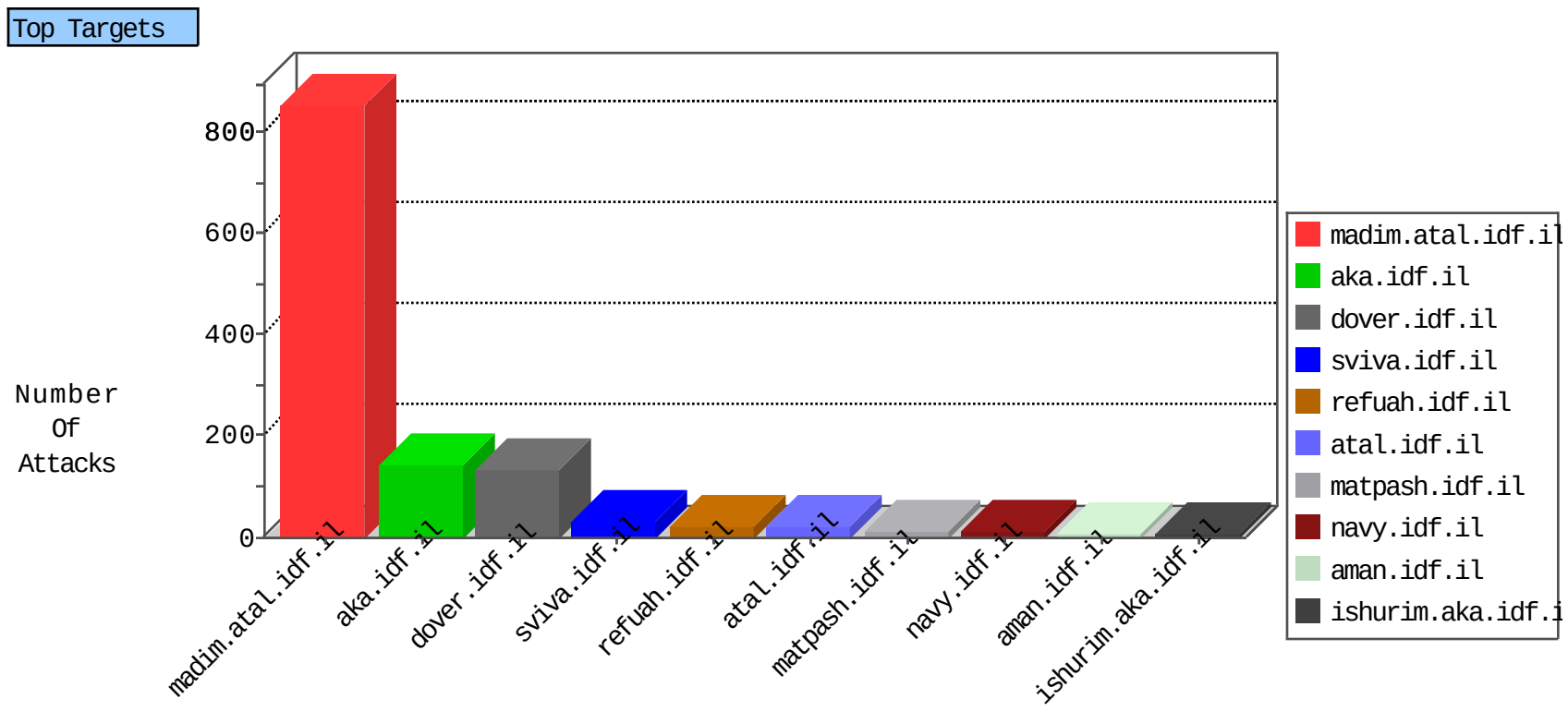
03-29-2015-09:03:03 to 03-29-2015-10:03:03

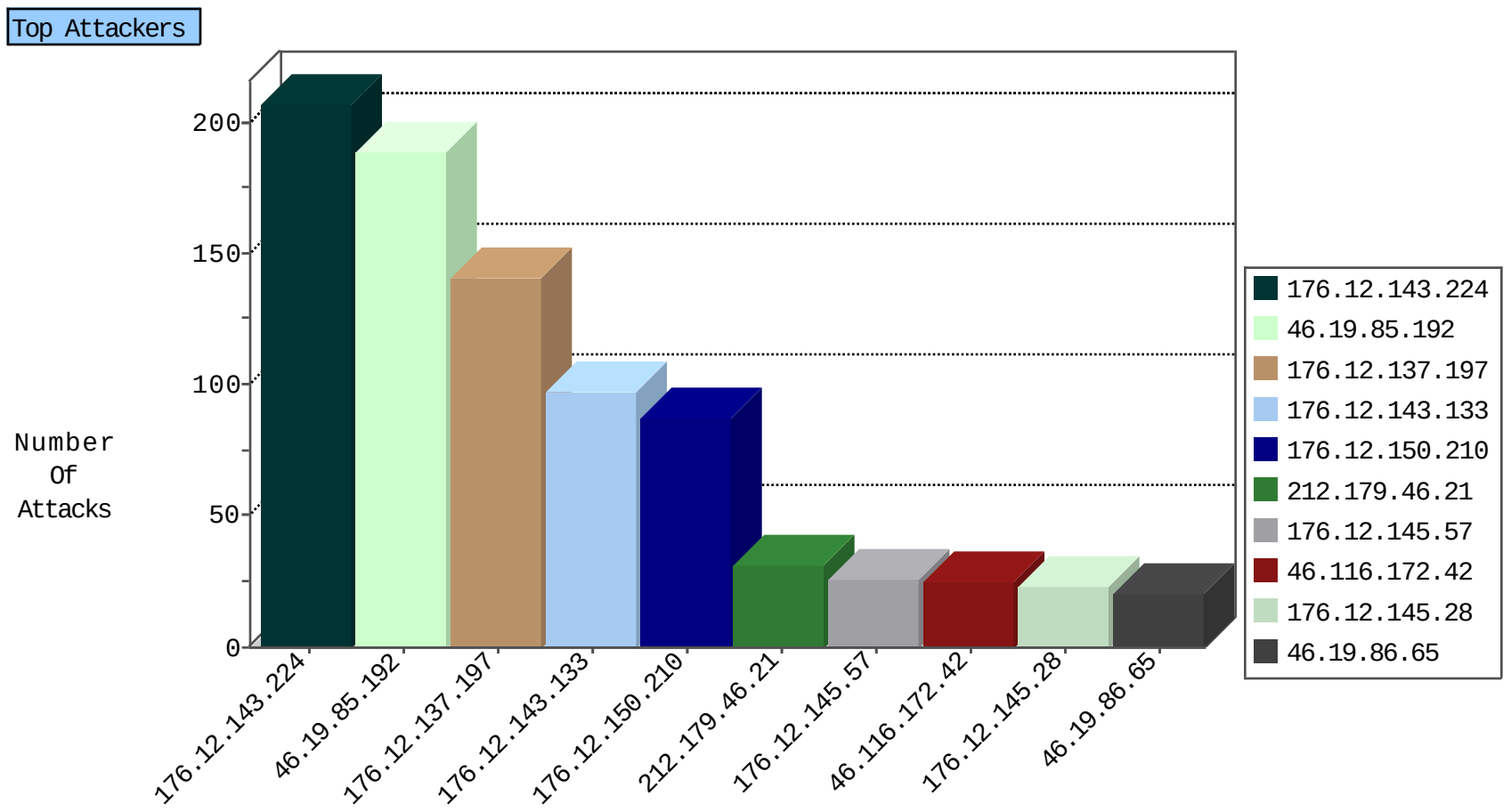
IDF Under Attack
03-29-2015-09:03:03

Top Targets



Top Target

Top Attackers



Top Attackers

03-29-2015-09:03:03 to 03-29-2015-10:03:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count

03-29-2015-09:03:03 to 03-29-2015-10:03:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
77.127.132.2	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
79.182.180.11	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
37.26.147.216	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
94.230.93.220	Israel	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	1
104.246.70.193		147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
77.127.248.167	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
109.64.166.232	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
178.217.187.39	Poland	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
94.230.93.179	Israel	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
46.121.64.222	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

03-29-2015-09:03:03 to 03-29-2015-10:03:03

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	4
62.90.234.5	Israel	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
66.249.64.10	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	1
212.179.46.16	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.161.221	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
196.47.173.21	Cote D'Ivoire	147.237.76.148	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 4096	1
62.90.234.5	Israel	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
185.32.178.13	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
62.90.234.5	Israel	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
182.92.236.44	China	147.237.8.14	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.11	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
176.12.138.45	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.165	Japan	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
109.253.134.34	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.165	Japan	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
109.65.58.171	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.186.131	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
84.228.16.125	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.30.205	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
62.219.210.125	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
208.39.68.33	United States	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
62.90.234.5	Israel	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
182.92.236.44	China	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
176.12.145.168	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.109	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.144.142	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
43.255.191.165	Japan	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
109.66.2.171	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.162.65	Israel	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
94.249.46.219	Jordan	147.237.77.216	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.132.192	Israel	147.237.72.166	aka.idf.il	portscan: TCP Distributed Portscan	1

03-29-2015-09:03:03 to 03-29-2015-10:03:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.46.21	Israel	147.237.77.235	sviva.idf.il	First packet isn't SYN	drop	drop	31
109.253.141.206	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
46.19.85.164	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	8
62.210.141.227	France	147.237.77.176	matpash.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	8
185.32.176.116	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
46.19.85.69	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
109.253.142.168	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
46.19.85.128	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid ACK number	Bad TCP sequence	monitor	6
187.217.112.50	Mexico	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	6
134.191.232.69	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
213.244.84.242	Palestinian Territory, Occupied	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
46.19.85.248	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
109.253.142.105	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
17.142.152.72	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
17.142.152.86	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
5.102.254.77	Israel	147.237.72.156	aman.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
46.19.86.171	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
62.0.212.217	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	3
80.179.115.198	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
188.120.148.129	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
2.54.183.253	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
2.54.186.131	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	2
46.116.172.42	Israel	147.237.0.19	madim.atal.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
2.52.11.54	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	2
157.55.39.42	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
2.54.183.253	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
157.55.39.67	United States	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	2
2.54.183.253	Israel	147.237.72.166	aka.idf.il	Invalid sequence number	Bad TCP sequence	monitor	2
62.0.211.155	Israel	147.237.72.156	aman.idf.il	First packet isn't SYN	drop	drop	2
46.19.86.131	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
207.46.13.5	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
2.54.186.131	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
2.52.11.54	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
80.179.115.198	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
46.19.85.205	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
2.54.186.131	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
2.52.11.54	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
46.19.85.10	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.86.143	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
176.12.150.144	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
66.249.81.220	United States	147.237.76.200	eitan.aka.idf.il		drop	drop	1
212.117.143.250	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
185.32.176.41	Israel	147.237.72.156	aman.idf.il	Invalid sequence number	Bad TCP sequence	monitor	1
46.19.86.60	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.85.175	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
80.246.136.25	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1

03-29-2015-09:03:03 to 03-29-2015-10:03:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
176.12.143.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	207
46.19.85.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	188
176.12.137.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	141
176.12.143.133	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	97
176.12.150.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	87
176.12.145.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	26
176.12.145.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	23
46.116.172.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	23
46.19.86.65	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	20
176.12.150.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	18
37.26.146.135	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	17
62.0.102.190	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	10
77.127.248.167	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	6
109.65.6.41	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	5
31.168.89.122	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 31.168.89.122	Block	3
207.46.13.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.112	Block	3
132.66.164.253	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
132.72.132.128	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	3
176.12.150.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2
81.218.181.239	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
185.32.176.116	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.64.112.84	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
37.26.147.154	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
132.75.160.243	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
77.127.248.167	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	2
85.95.255.158	Turkey	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 85.95.255.158	Block	2
157.55.39.6	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.6	Block	2
207.46.13.16	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.16	Block	2
109.65.164.235	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.42	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.42	Block	2
31.168.89.122	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	2
77.126.175.207	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.182.180.11	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	2
89.234.68.90	Ireland	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	2
109.253.130.72	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.166	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
188.165.15.196	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
46.117.159.7	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/modiin/default.aspx	Block	1
87.68.211.57	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/declarationofemployment.aspx	None	1
5.255.253.16	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/faq/stylesheet	Block	1
207.46.13.5	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.253.145.109	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.228.200.252	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
216.218.206.67	United States	147.237.76.39	mobile.meitav.idf.i	Unauthorized URL Access to 147.237.76.39/	Block	1
109.253.139.32	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//dover/site/mainpage.asp	Block	1
66.249.78.173	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	1
188.165.15.196	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.196	Block	1
46.120.235.219	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
87.69.1.249	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1

03-29-2015-09:03:03 to 03-29-2015-10:03:03