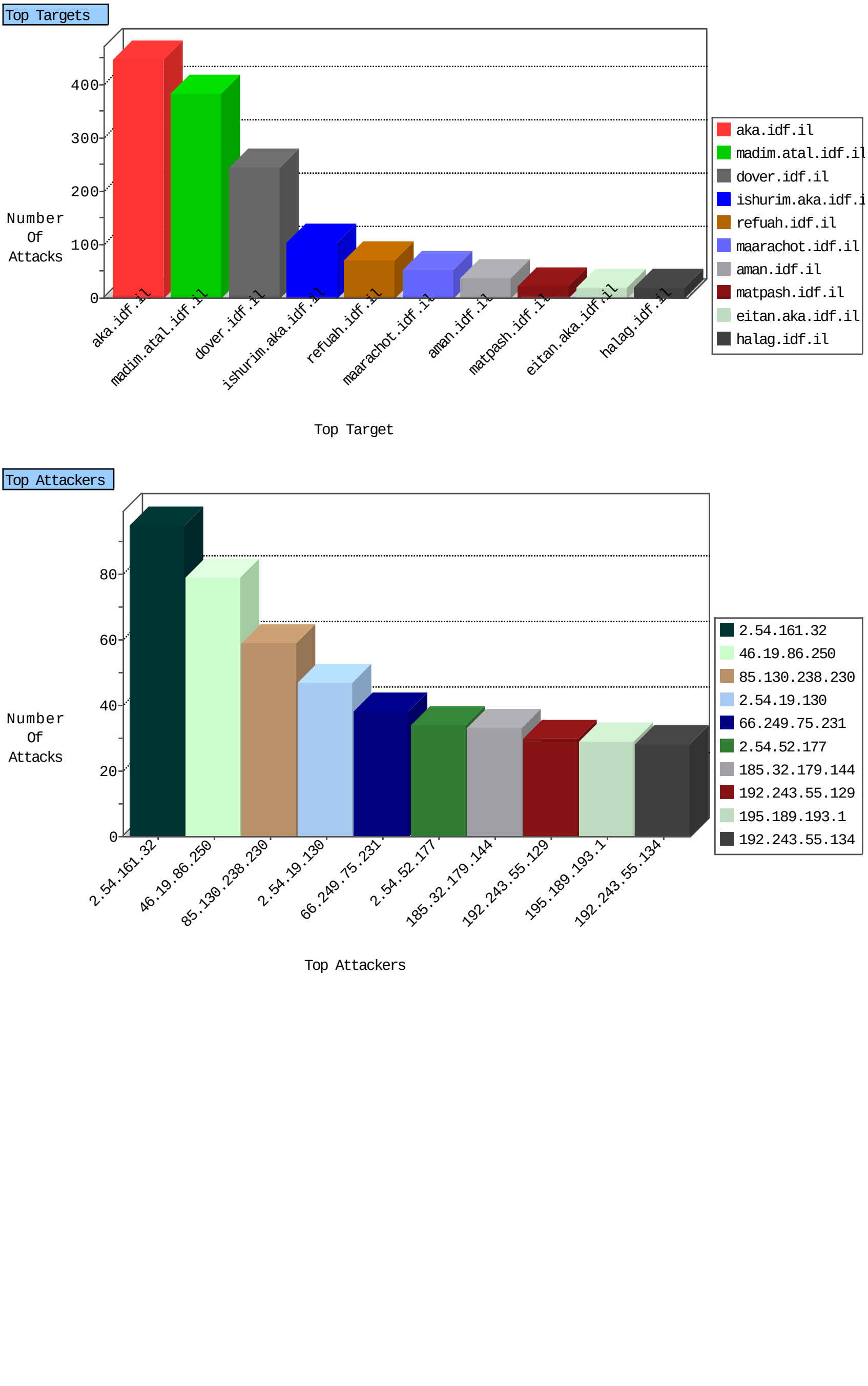
02-21-2016-11:04:00 to 02-21-2016-12:04:00

IDF Under Attack Daily Report



02-21-2016-11:04:00 to 02-21-2016-12:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.93.154.216	United States	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	195
84.111.65.41	Israel	147.237.77.74	law.idf.il	Block_Udp_All_Nets	drop	3
134.147.203.115	Germany	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	2
185.94.111.1		147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

02-21-2016-11:04:00 to 02-21-2016-12:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.130.224	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	6
5.29.84.165	Israel	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	2
157.55.39.216	United States	147.237.0.34	tikshuv.idf.il	C1000212: HTTP: prefix 1.01 in the URL	Block	1
188.165.15.214	France	147.237.76.147	chinuch.aka.idf.il	C1000228: HTTP: AhrefBot crawler	Block	1

02-21-2016-11:04:00 to 02-21-2016-12:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.75.231	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	38
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
2.54.157.193	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.88.81.30	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.44.133.108	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.76.31	China	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
79.182.107.134	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
216.72.40.185	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.159	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.25.106.78	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.68	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	1
37.26.147.130	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.249	147.237.76.86		navy.idf.il	ET SCAN NMAP -sS window 1024	1
2.54.187.152	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.54	147.237.76.44		e.refuah.idf.il	ET SCAN Potential SSH Scan	1
109.66.7.184	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
88.249.106.23	147.237.72.14	Turkey	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
217.194.203.52	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.102.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.240.201	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.116.63.213	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.199.57.196	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.42	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.110.40.7	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.46.39.136	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.116.94.110	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.8.88.245	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
185.110.132.54	147.237.76.198		e.yohalan.idf.il	ET SCAN Potential SSH Scan	1

02-21-2016-11:04:00 to 02-21-2016-12:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
85.130.238.230	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	59
195.189.193.1	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	29
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	26
79.178.200.40	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
176.13.21.80	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
80.246.130.93	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	17
212.76.127.10	Israel	147.237.77.234	halag.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	15
46.120.70.96	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
66.102.9.76	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	14
212.117.136.6	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
84.111.113.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
80.82.64.220	Netherlands	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
176.13.6.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
81.218.66.107	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.222	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.181.106.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
2.54.52.177	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
84.110.109.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.221.64	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.176	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.153	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.67.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
79.182.203.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.120.148.228	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.0.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.88.24.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.219.236.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.177.62.160	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.19.142	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.219.118.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.137.1	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.86	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
80.246.137.1	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
85.65.217.122	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.86	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.137.1	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.210.186.45	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.21	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
85.130.244.240	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

02-21-2016-11:04:00 to 02-21-2016-12:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.161.32	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	72
46.19.86.250	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	67
2.54.19.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	47
185.32.179.144	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	33
2.54.52.177	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	28
46.19.86.128	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	25
2.54.161.32	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	23
5.29.146.44	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 5.29.146.44	Block	22
2.54.41.194	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	17
2.52.166.103	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
46.19.86.250	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	12
176.13.0.208	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	11
149.88.24.225	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	9
176.13.18.186	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.19.86.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.142.6	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
80.246.139.233	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.52.178.40	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/admin	Block	2
2.54.173.231	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
157.55.39.222	United States	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.116.39.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
37.26.148.222	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
66.249.75.150	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
185.32.179.199	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
84.108.33.168	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
2.54.162.233	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
192.115.90.150	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/113535.pdf	Block	1
87.70.3.176	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
79.182.142.88	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
46.19.85.189	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Illegal Byte Code Character in Method	Block	1
70.35.201.207	United States	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
109.253.207.109	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
46.121.77.59	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
207.46.13.167	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/modiin/modiin/modiin/default.aspx	Block	1
81.218.251.250	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	1
176.13.18.186	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
37.26.147.237	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyuss	Block	1
169.229.3.91	United States	147.237.76.31	nakchal.idf.il	Malformed URL	Block	1
79.177.174.224	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
213.57.183.133	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	1
141.212.122.129	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to /x	Block	1
197.36.250.183	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
2.52.178.40	Israel	147.237.77.233	atal.idf.il	Admin Blocking	Block	1
95.30.38.195	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation &l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
79.182.204.39	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
46.19.85.189	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
173.214.173.238	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
70.35.201.207	United States	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1

02-21-2016-11:04:00 to 02-21-2016-12:04:00