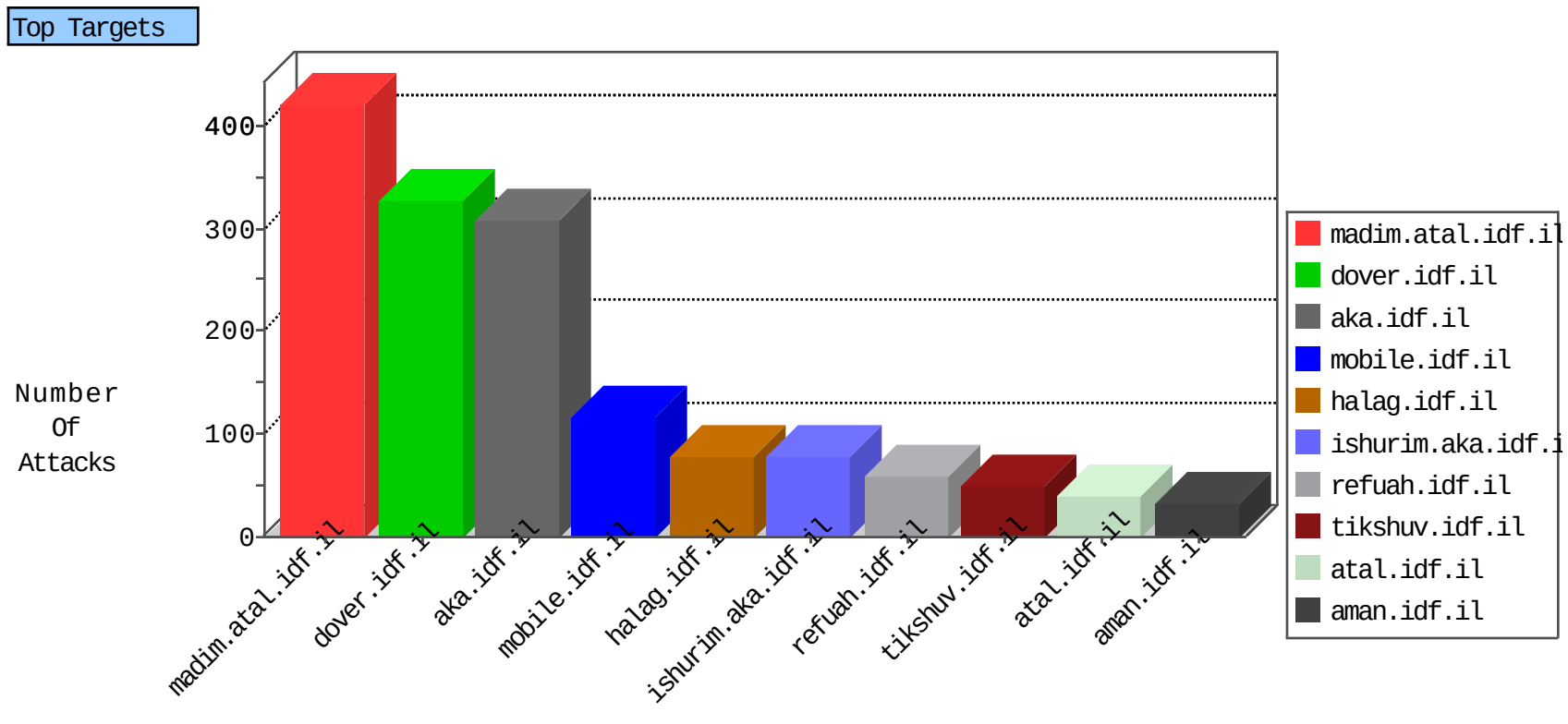
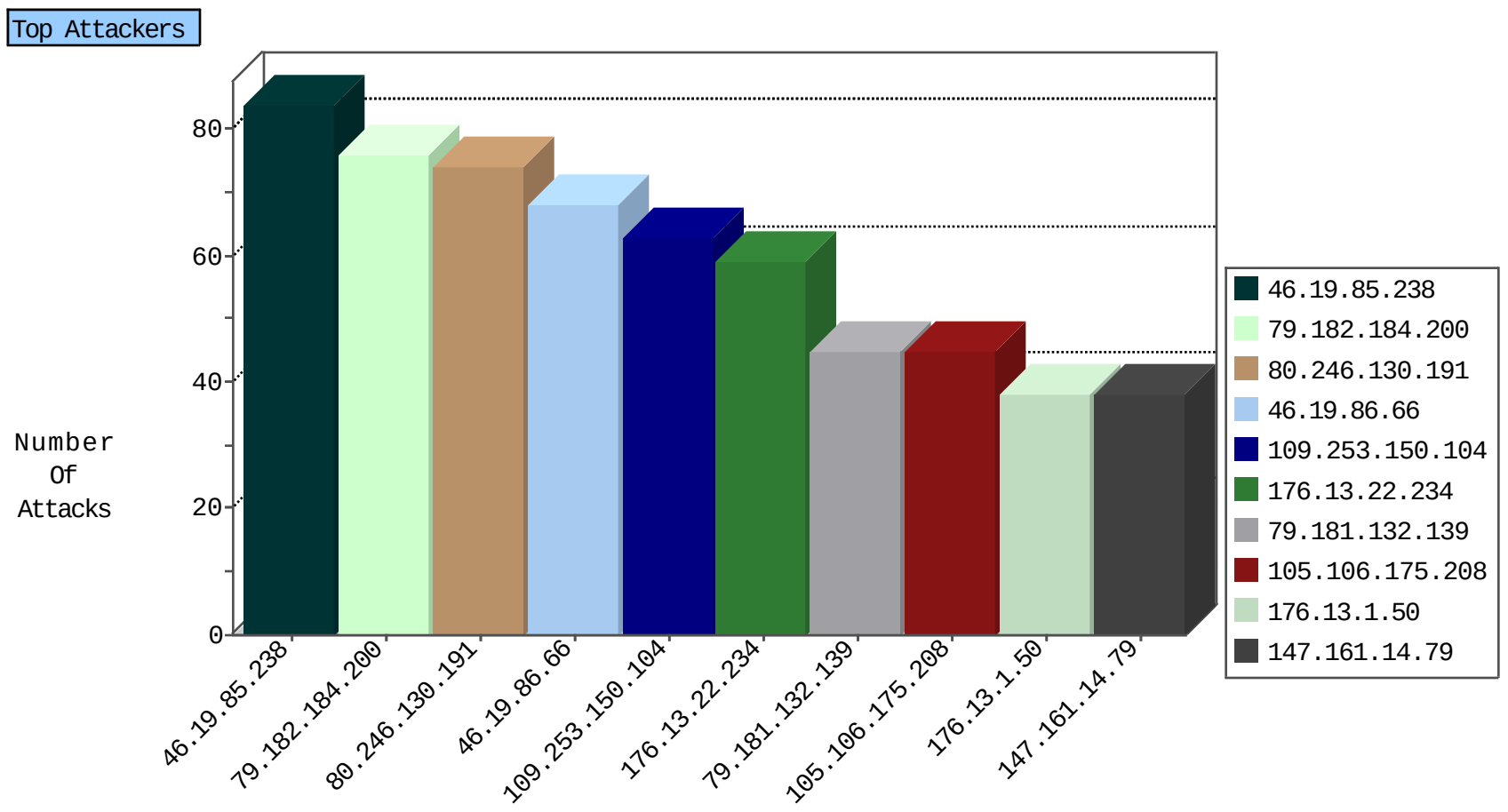
02-28-2016-10:04:02 to 02-28-2016-11:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-28-2016-10:04:02 to 02-28-2016-11:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.132.139	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	27
79.181.132.139	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	15
147.235.8.31	Israel	147.237.77.216	dover.idf.il	L4 Source or Dest Port Zero	drop	6
79.181.132.139	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
115.239.228.10	China	147.237.0.34	tikshuv.idf.il	JLM_Under_Attack_Con_Http	drop	2
115.239.228.10	China	147.237.0.34	tikshuv.idf.il	JLM_Purple_Con_Limit_Http	drop	1
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	1
80.246.136.132	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

02-28-2016-10:04:02 to 02-28-2016-11:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.235.31.129	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.181.102.173	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
109.65.82.168	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
62.90.182.151	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
192.114.23.208	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
37.26.148.129	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
109.67.150.105	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
51.255.65.97	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.8	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
109.253.129.8	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
51.255.65.47	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.13	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.55	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.19	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.64	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.37	United Kingdom	147.237.77.170	maarachot.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.80	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.39	United Kingdom	147.237.77.74	law.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

02-28-2016-10:04:02 to 02-28-2016-11:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
213.57.42.100	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.23.247	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
147.235.185.74	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.113.125.11	147.237.77.243	Romania	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
82.102.169.113	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.178.121.228	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -sS window 1024	1
54.72.0.55	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	1
217.216.140.66	147.237.76.31	Spain	nakchal.idf.il	ET SCAN Potential SSH Scan	1
37.26.147.242	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.216.140.66	147.237.72.14	Spain	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
31.168.151.22	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.199.244.112	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.1.236	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.90.79.80	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.193	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1
90.154.239.123	147.237.77.216	Bulgaria	dover.idf.il	portscan: TCP Distributed Portscan	1
80.178.187.231	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
60.217.72.16	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
217.216.140.66	147.237.77.235	Spain	sviva.idf.il	ET SCAN Potential SSH Scan	1
37.46.41.89	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.216.140.66	147.237.72.156	Spain	aman.idf.il	ET SCAN Potential SSH Scan	1
37.26.147.221	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-28-2016-10:04:02 to 02-28-2016-11:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.246.130.191	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	73
147.161.14.79	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	26
176.13.23.161	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
192.115.177.202	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	22
212.179.46.16	Israel	147.237.76.197	e.himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	20
176.13.20.39	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
80.246.135.51	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
109.65.5.50	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
2.54.27.249	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
109.253.159.216	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.129.216	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.137.26	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.24.102	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
185.81.43.203		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
80.179.114.27	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
62.90.131.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.252	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.159.169.181	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.14	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.219.163.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.47.38	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.86.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.198.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
73.138.210.67	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.230	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
64.236.4.1	United States	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
185.32.179.112	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.26.148.204	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
208.109.97.62	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.52.42.213	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.26.188	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
31.154.3.195	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.142	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.17	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.21.31	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.151	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
193.33.2.114	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.237	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	4
80.179.114.27	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
91.197.61.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.151	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
167.220.196.87	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.81.43.203		147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
37.26.149.177	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
199.203.215.1	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.17	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
79.177.42.39	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-28-2016-10:04:02 to 02-28-2016-11:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.238	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	84
79.182.184.200	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	76
46.19.86.66	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	67
109.253.150.104	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	63
176.13.22.234	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	59
176.13.1.50	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	38
80.246.136.25	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
192.115.177.202	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.115.177.202	Block	14
66.249.79.75	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.75	Block	10
176.13.7.46	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter NewPassword	Block	8
176.13.11.78	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
192.115.252.2	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.115.252.2	Block	8
105.106.175.208	Algeria	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	6
105.106.175.208	Algeria	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	6
105.106.175.208	Algeria	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-he/dover.aspx	Block	6
105.106.175.208	Algeria	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1362-he/dover.aspx	Block	5
105.106.175.208	Algeria	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1380-he/dover.aspx	Block	5
2.54.24.102	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
109.253.129.216	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
105.106.175.208	Algeria	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	Block	4
192.115.252.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	3
109.253.145.17	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	3
109.253.204.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
212.150.245.250	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized HTTP Method	Block	3
2.54.22.241	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
82.80.198.164	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	3
2.54.53.36	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.54.53.36	Block	2
78.224.131.96	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.253.203.114	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.54.36.113	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
81.218.70.243	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	2
212.150.245.250	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 212.150.245.250	Block	2
109.253.159.216	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
105.106.175.208	Algeria	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucArticleLobbyControl$datepicker in www.idf.il/1380-he/dover.aspx	Block	1
66.249.66.33	United States	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
185.37.12.200	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
40.77.167.104	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
167.220.196.87	United Kingdom	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.146.238	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.207.243	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter NewPassword	Block	1
81.218.70.243	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.70.243	Block	1
212.150.245.250	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/8/	Block	1
77.127.189.120	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
192.115.252.2	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1
8.37.233.169	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.65.5.50	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
46.19.86.66	Israel	147.237.0.19	madim.atal.idf.i	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	1
105.106.175.208	Algeria	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1785-he/dover.aspx	Block	1
82.166.146.115	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
217.194.203.52	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1

02-28-2016-10:04:02 to 02-28-2016-11:04:02