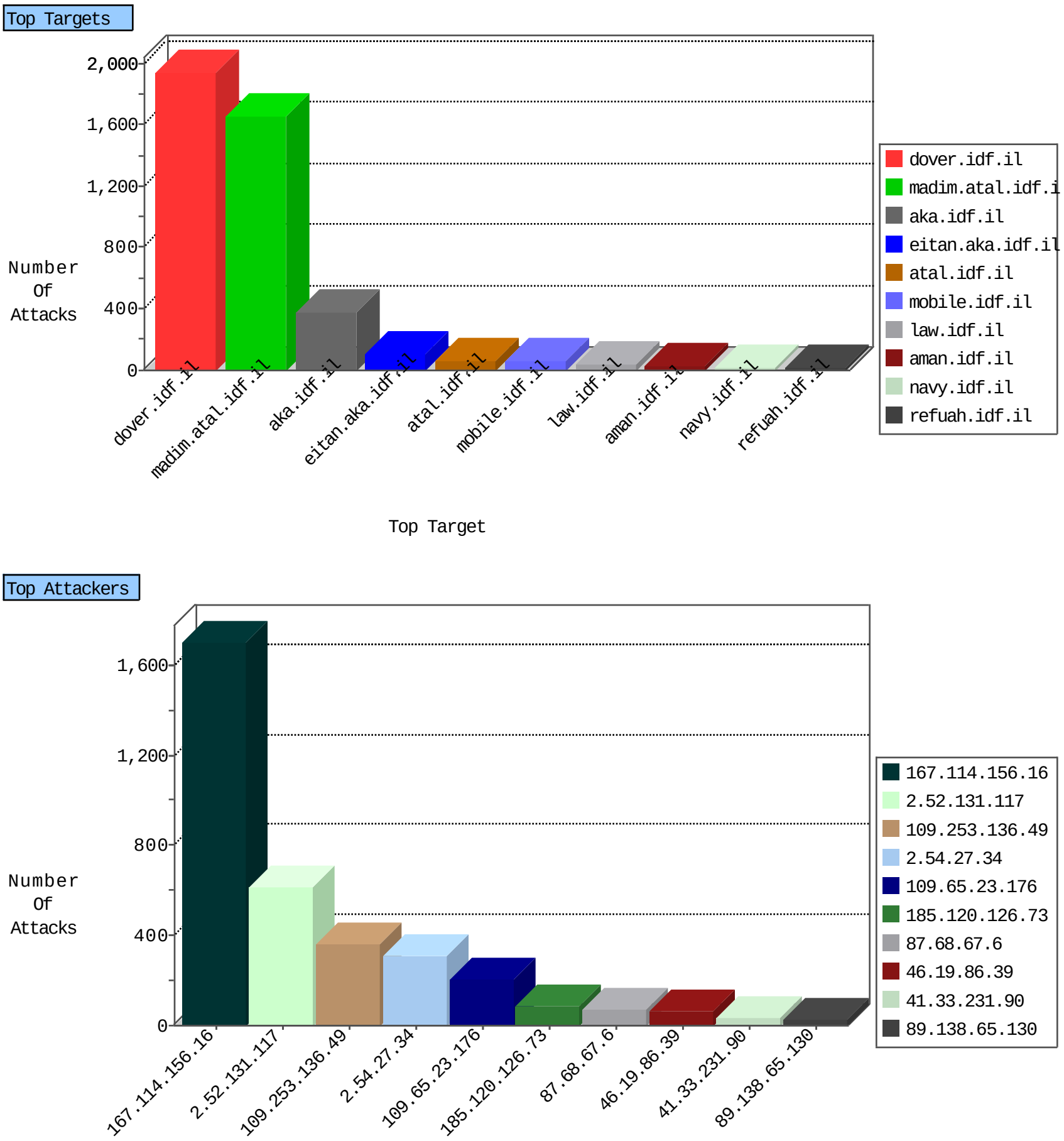
01-05-2016-21:04:05 to 01-05-2016-22:04:05

IDF Under Attack Daily Report



01-05-2016-21:04:05 to 01-05-2016-22:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3088
50.205.69.2	United States	147.237.76.147	chinuch.aka.idf.il	TCP handshake violation, first packet not syn	drop	2933
82.81.15.102	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3

01-05-2016-21:04:05 to 01-05-2016-22:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-05-2016-21:04:05 to 01-05-2016-22:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.130.151	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	9
66.249.81.139	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
66.249.81.135	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
87.68.240.218	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
36.72.228.72	147.237.76.201	Indonesia	e.atal.idf.il	ET SCAN NMAP -sS window 2048	1
52.90.147.148	147.237.77.179	United States	e.mazi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
209.126.116.147	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
46.228.207.18	147.237.77.243	Germany	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.252.84	147.237.72.217	China	e.idf.il	ET SCAN NMAP -sS window 3072	1
46.228.207.18	147.237.77.212	Germany	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.252.84	147.237.72.217	China	e.idf.il	ET SCAN NMAP -f -sS	1
46.228.207.18	147.237.76.200	Germany	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.186.163.12	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.228.207.18	147.237.72.156	Germany	aman.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.162.131	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential SSH Scan	1
36.72.228.72	147.237.76.201	Indonesia	e.atal.idf.il	ET SCAN NMAP -sS window 3072	1
84.228.221.193	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
36.72.228.72	147.237.76.201	Indonesia	e.atal.idf.il	ET SCAN NMAP -f -sS	1
79.176.26.52	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.12.39.85	147.237.77.19	Russian Federation	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
46.228.207.18	147.237.77.243	Germany	mobile.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
209.126.116.147	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
46.228.207.18	147.237.77.233	Germany	atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.252.84	147.237.72.217	China	e.idf.il	ET SCAN NMAP -sS window 2048	1
46.228.207.18	147.237.77.61	Germany	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
46.228.207.18	147.237.72.167	Germany	ishurim.aka.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
106.75.199.201	147.237.8.46	China	e.chinuch.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
46.228.207.18	147.237.0.35	Germany	akaws.idf.il	ET SCAN NMAP -sS window 1024	1

01-05-2016-21:04:05 to 01-05-2016-22:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
87.68.67.6	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	69
185.120.126.73		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	56
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
185.120.126.73		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	27
79.180.7.73	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	24
46.210.191.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.120.238.81	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
130.219.8.11	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	14
84.111.28.61	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
188.120.159.233	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.160.132.211	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.178	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.246.130.151	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
79.180.1.166	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
79.177.21.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
5.102.253.12	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
80.246.130.151	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
94.230.86.162	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
109.253.215.190	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
79.177.1.194	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
109.253.215.190	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.221	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
217.132.135.246	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.221	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
107.170.20.192	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.132.135.246	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.67.130.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.16.95	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.250.228.91	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
46.19.86.26	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
85.250.228.91	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
85.250.228.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.54.172.95	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.26.147.244	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence		alert	4
212.179.21.194	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
130.193.51.104	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
109.160.132.211	Israel	147.237.0.19	madim.atal.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
213.8.204.71	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
84.109.235.237	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
31.210.187.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
87.69.210.74	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.107	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.26.147.244	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
31.210.188.35	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.67.149.213	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.217.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.108.240.132	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.65.63.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.52.32	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	3

01-05-2016-21:04:05 to 01-05-2016-22:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.131.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	312
2.52.131.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	258
109.253.136.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	174
2.54.27.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	151
2.54.27.34	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 2.54.27.34	Block	111
109.65.23.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	111
109.253.136.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
109.65.23.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	97
46.19.86.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
2.54.27.34	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.54.27.34	Block	46
2.52.131.117	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	42
109.253.136.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	32
89.138.65.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
84.228.13.21	Israel	147.237.72.166	aka.idf.il	Too Many of the Same Response Code (404) in Session from 84.228.13.21	Block	24
2.54.34.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
79.178.60.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
149.78.50.201	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 149.78.50.201	Block	10
109.64.210.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
85.250.233.231	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	9
109.253.157.71	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/sachar/forgotpassword.aspx parameter	None	4
2.52.131.117	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	4
46.120.142.235	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
85.64.96.55	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
46.19.86.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.133	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 37.26.149.133	Block	3
80.246.136.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.130.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.15.189	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
37.26.147.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
95.187.76.124	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/ https:/youtu.be/g5y1kierpl0	Block	2
114.97.49.4	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 114.97.49.4	Block	2
188.165.89.85	France	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	2
2.54.181.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.149.133	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1431	Block	2
188.165.89.85	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
185.32.179.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
192.116.55.92	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mobile/main/giyus/general.aspx	Block	1
176.13.9.157	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.213.40	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.139.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.8.204.39	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.28.173.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
94.230.86.162	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.153	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m/main/smalim/smalim.aspx	Block	1
185.120.125.25		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.228.13.21	Israel	147.237.72.166	aka.idf.il	Too Many 404: Response Code per Session	Block	1
54.183.120.101	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1

01-05-2016-21:04:05 to 01-05-2016-22:04:05