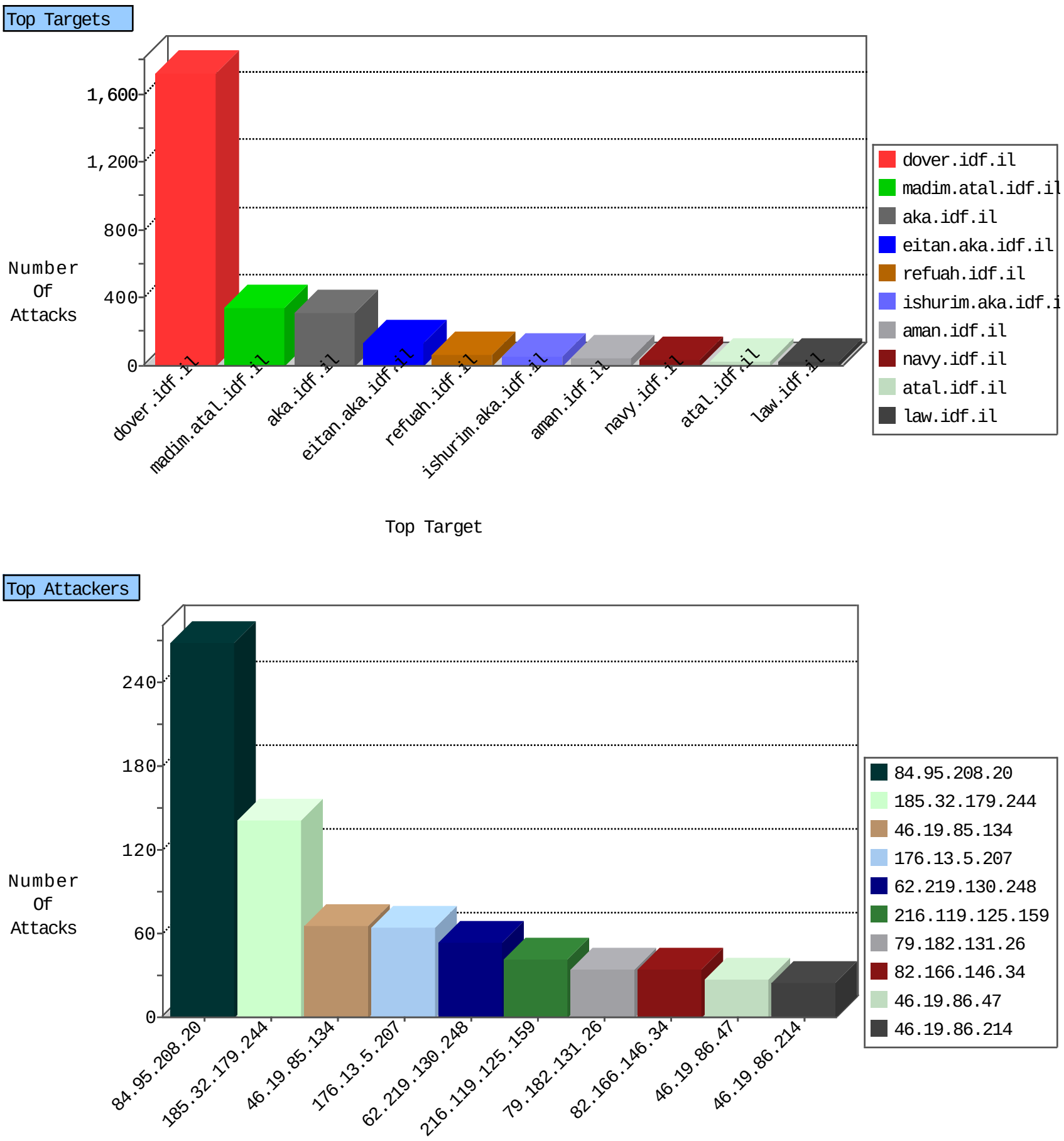
09-19-2016-11:04:00 to 09-19-2016-12:04:00

IDF Under Attack Daily Report



09-19-2016-11:04:00 to 09-19-2016-12:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.6.200	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
84.52.98.134	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	6
37.46.39.225	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
130.217.77.4	New Zealand	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	3
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Black List	drop	3
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
200.19.159.35	Brazil	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
60.173.14.92	China	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Http	drop	1
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.82	Czech Republic	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
129.97.74.12	Canada	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.206.158.138	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.22.150.78	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.42.142.45	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
40.77.167.21	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

09-19-2016-11:04:00 to 09-19-2016-12:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.151.208.90	United Kingdom	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
216.119.125.159	United States	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
216.119.125.159	United States	147.237.72.166	aka.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4

09-19-2016-11:04:00 to 09-19-2016-12:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
216.119.125.159	147.237.72.166	United States	aka.idf.il	SQL Injection - Select From	33
91.151.208.90	147.237.72.166	United Kingdom	aka.idf.il	SQL Injection - Select From	18
2.55.34.187	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.97.30	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.32.221	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.50	147.237.72.217	Ukraine	e.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
213.8.204.61	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.0.210	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
88.249.106.23	147.237.76.148	Turkey	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
200.195.135.82	147.237.77.176	Brazil	matpash.idf.il	ET SCAN NMAP -sS window 3072	1
77.139.54.204	147.237.72.166	France	aka.idf.il	portscan: TCP Distributed Portscan	1
177.200.192.51	147.237.77.205	Brazil	prisha.idf.il	ET SCAN NMAP -sS window 4096	1
66.249.66.131	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
177.200.192.51	147.237.77.205	Brazil	prisha.idf.il	ET SCAN NMAP -f -sS	1
62.219.147.212	147.237.77.176	Israel	matpash.idf.il	ET SCAN NMAP -sA (2)	1
154.16.199.175	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
62.90.2.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
113.240.250.154	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
2.55.159.230	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.55.146	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.133.72	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.50	147.237.72.217	Ukraine	e.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.20.180	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
200.195.135.82	147.237.77.176	Brazil	matpash.idf.il	ET SCAN NMAP -sS window 4096	1
82.80.163.222	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.137	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.126.4.139	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
177.200.192.51	147.237.77.205	Brazil	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
62.219.162.101	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
154.16.199.175	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
62.219.125.109	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
141.226.217.129	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.182	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.130.14	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

09-19-2016-11:04:00 to 09-19-2016-12:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
79.182.131.26	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	34
37.46.33.27	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	24
139.130.188.222	Australia	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	24
132.71.141.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
46.19.85.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.85.134	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
46.19.85.134	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
2.55.168.104	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
87.68.46.255	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
2.53.156.81	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.19.86.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
176.13.244.33	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
109.253.228.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
109.253.192.67	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
46.19.86.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
176.13.1.114	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
31.210.187.43	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.53.9.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.55.16.247	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.0	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
176.13.225.109	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
176.13.17.54	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
79.179.60.242	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
152.62.109.207	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
89.139.202.174	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
176.13.1.8	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.53.191.93	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.53.41.152	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
2.55.135.7	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.55.147.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.55.143.103	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
62.0.216.189	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
66.220.145.246	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
62.0.214.129	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
79.177.178.28	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.55.148.104	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
85.65.188.154	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
176.13.13.176	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
37.26.149.152	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.53.161.13	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.143.161.163	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.55.172.178	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
2.53.36.78	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
81.218.204.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.220.145.243	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7

09-19-2016-11:04:00 to 09-19-2016-12:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	141
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	101
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	84
176.13.5.207	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	63
62.219.130.248	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/	Block	54
82.166.146.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
46.19.86.47	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
80.246.139.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
80.246.139.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
80.246.136.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
46.19.85.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
213.244.105.5	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	8
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	8
46.19.85.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
213.244.105.5	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1153-17675-en/	Block	7
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	6
82.80.26.168	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized HTTP Method	Block	5
79.176.56.247	Israel	147.237.76.42	refuah.idf.il	Unauthorized HTTP Method	Block	5
213.244.105.5	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1153-17675-en/dover.aspx - in 2012 idfcalled baha abu al ata, a member of the higher military council and commander of islamic jihad gaza city brigade confirm date in news.	Block	3
109.253.147.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.80.26.168	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/sip_storage/files/8/	Block	3
109.253.158.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
213.244.105.5	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1153-17675-en/dover.aspx - in 2012 idfcalled baha abu al ata, a member of the higher military council and commander of islamic jihad gaza city brigade. confirm date in news.	Block	3
79.176.56.247	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/sip_storage/files/3/	Block	3
109.253.204.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	2
85.114.106.248	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	2
176.13.250.181	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.55.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation aspxerrorpath in www.idf.il/error.htm	Block	2
85.114.106.248	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1153-17675-en/	Block	2
2.53.153.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.142.191.167	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
176.13.5.207	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEntrance in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	1
81.218.59.82	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1250-he/atal.aspx	Block	1
77.139.120.230	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/	Block	1
109.64.187.44	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
46.19.86.229	Israel	147.237.76.86	navy.idf.il	Distributed Unknown HTTP Request Method	Block	1
89.237.127.31	France	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.64	Israel	147.237.76.42	refuah.idf.il	Illegal HTTP Version _pk_id.118.fd1c=fa6911641ab9c789.1449477969.5.1463380872.1463380645.	Block	1
202.155.58.28	Indonesia	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/cgi-bin/webcgi/login	Block	1
31.154.19.5	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 31.154.19.5	Block	1
117.78.13.18	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/robots.txt	Block	1
104.61.36.245	United States	147.237.76.39	mobile.meitav.idf.i	Illegal Byte Code Character in Method q[[#0]][[#0]][[#0]]A÷[[#15]]È‹žgj{[[#24]]FÔ´ÎÙúÄ™_šèd)rœhüŸ#[[#7]]9ŽSpÒ`À2b-&•ÍVLq[[#26]]Ñr©[[#3]]a[[#24]]¹pµíÄ”!`Ê~ÿ¸47Ý_[[#6]]Y\2åÃï4gPÔœ±à	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
46.19.86.19	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
84.108.238.1	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
40.77.167.16	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
176.13.11.161	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1

09-19-2016-11:04:00 to 09-19-2016-12:04:00