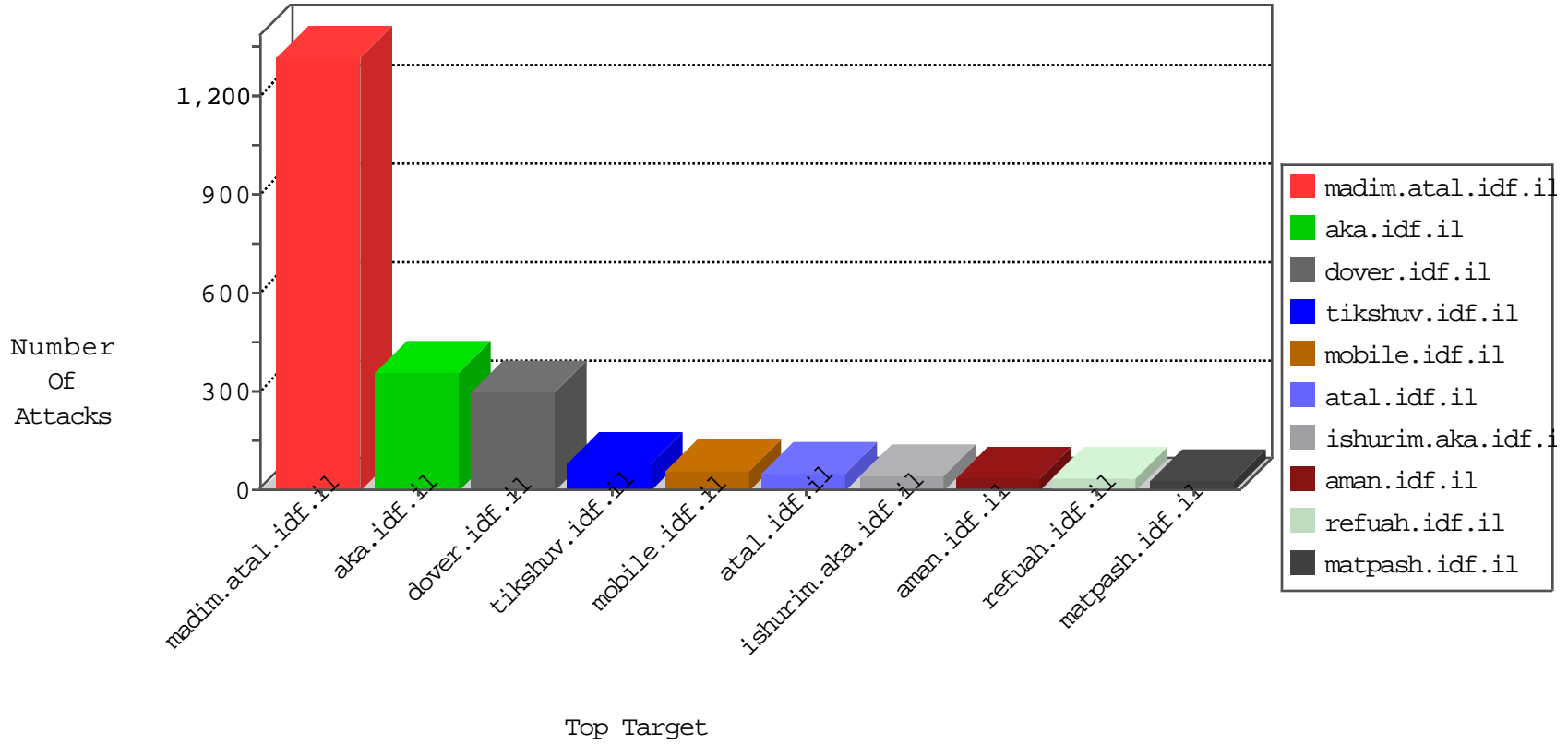


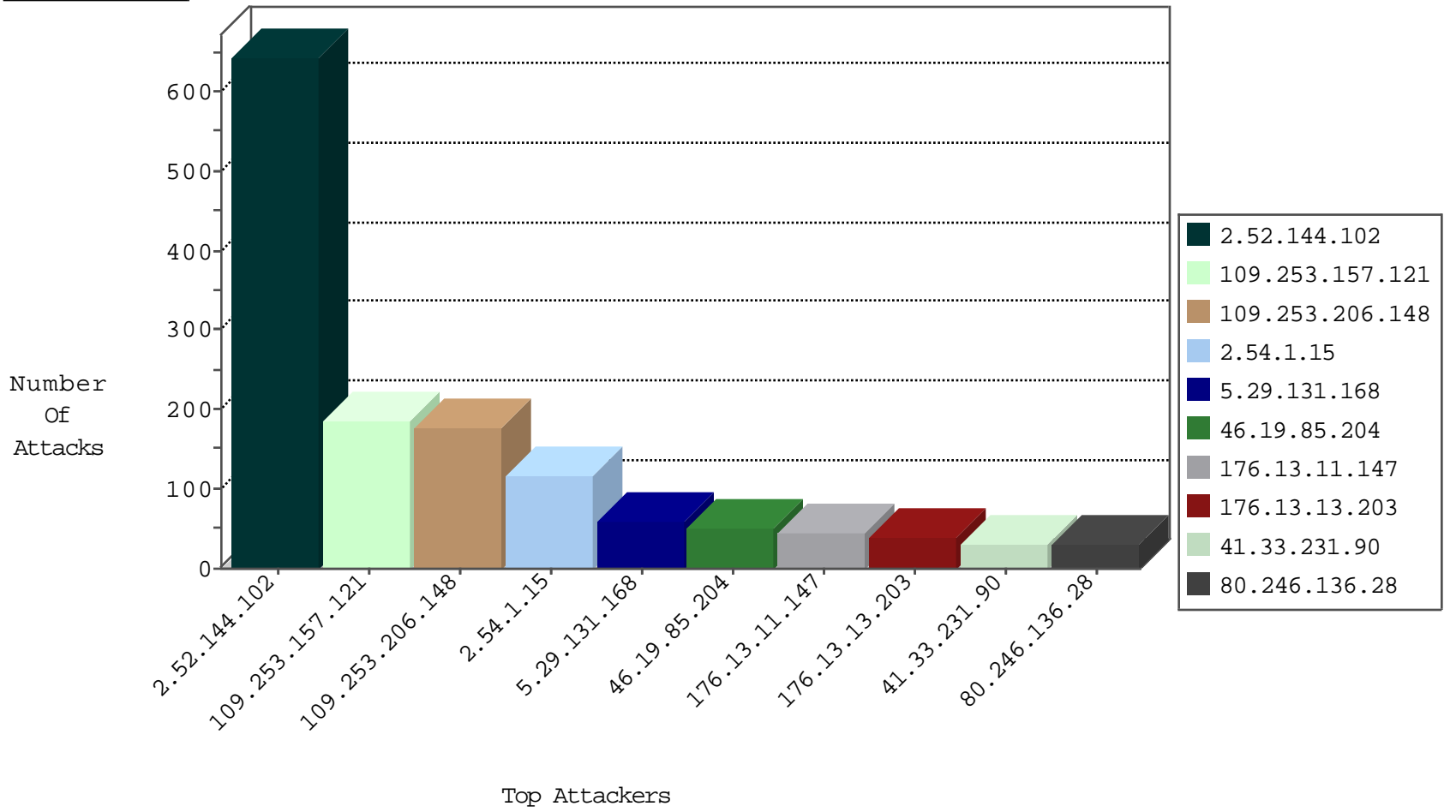
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	3156
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
82.81.12.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
159.104.163.19	United Kingdom	147.237.77.176	matpash.idf.il	Invalid TCP Flags	drop	1
183.56.159.141	China	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
82.145.33.11	United Kingdom	147.237.76.34	ychalan.idf.il	Block_Ip_Web_In	drop	1
159.104.163.21	United Kingdom	147.237.77.176	matpash.idf.il	Invalid TCP Flags	drop	1
142.54.169.162	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traffic	drop	1
159.104.163.22	United Kingdom	147.237.77.176	matpash.idf.il	Invalid TCP Flags	drop	1
159.104.163.18	United Kingdom	147.237.77.176	matpash.idf.il	Invalid TCP Flags	drop	1
176.13.11.147	Israel	147.237.0.19	madim.atal.idf.il	DOSS-SSL-ClearText	drop	1

01-27-2016-11:04:00 to 01-27-2016-12:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
31.61.140.88	Poland	147.237.77.176	matpash.idf.il	C008: HTTP: Xenu UserAgent	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
203.255.31.195	147.237.76.31	Korea, Republic of	nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
5.102.229.69	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
168.62.238.153	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.93.181	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
85.250.100.189	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.130.89	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.10.131	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.222	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.76.199	China	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
31.154.94.60	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
5.29.136.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
163.172.13.173	147.237.77.170	United Kingdom	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.93.181	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
84.108.69.192	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.6.122	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.19.161	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.240.213.93	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
31.168.239.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.19.85.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
148.177.129.211	Europe	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	24
84.228.13.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
46.19.85.167	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
46.19.85.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
176.13.1.156	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
5.43.204.194	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	13
207.232.29.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
176.13.2.217	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.129	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
62.219.62.164	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
195.212.29.185	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.54.37.207	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
196.202.145.100	Sudan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.185	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.32.207.103	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.185	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.25	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.166	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.182.5.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.157	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.61	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.205.189.129	United Arab Emirates	147.237.76.147	chinuch.aka.idf.il	drop	SAM rule	drop	6
46.19.85.166	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
149.50.87.28	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.25	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.149.245	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.61	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.166	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.176.153.182	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.65.42.230	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.95	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.0.208.1	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.153.182	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
132.64.212.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.96	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.65.196.63	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.46.39.24	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.39	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.32.207.103	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.102.254.62	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.183.9.196	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.244	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.26.146.148	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	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

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.144.102	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	367
2.52.144.102	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	142
2.52.144.102	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	135
109.253.157.121	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	111
109.253.206.148	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	91
109.253.206.148	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	86
109.253.157.121	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	75
2.54.1.15	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	64
5.29.131.168	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	54
2.54.1.15	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	52
176.13.11.147	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	41
176.13.13.203	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	38
80.246.136.28	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
2.52.23.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	19
31.168.239.42	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	16
176.13.1.173	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
46.19.86.198	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
109.66.211.46	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	7
37.26.146.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.19.86.85	Israel	147.237.76.42	refuah.idf.il	Distributed Parameter Type Violation on www.refua.atal.idf.il/1518-he/refuah.aspx parameter ct100\$ContentPlaceholder1\$txtContent	Block	5
2.52.20.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
2.52.149.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
176.13.11.147	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	4
79.178.190.252	Israel	147.237.76.86	navy.idf.il	Distributed PHP Attempt	Block	3
37.26.149.132	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.66.211.46	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/0/	Block	3
79.178.190.252	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	3
109.253.217.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.149.189	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.145.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.52.191.245	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
207.46.13.10	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.10	Block	2
109.66.51.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.54.44.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.85.85	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
31.154.25.98	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 31.154.25.98	Block	2
46.19.86.74	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.2.217	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.54.20.141	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
89.139.129.183	Israel	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
109.253.200.58	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.205.107	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
157.55.39.239	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.54.37.207	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.109	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
130.193.51.51	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.139.129.183	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Value	Block	1
81.165.102.157	Belgium	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
46.19.85.68	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$txtContent in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
14.158.254.1	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 14.158.254.1	Block	1