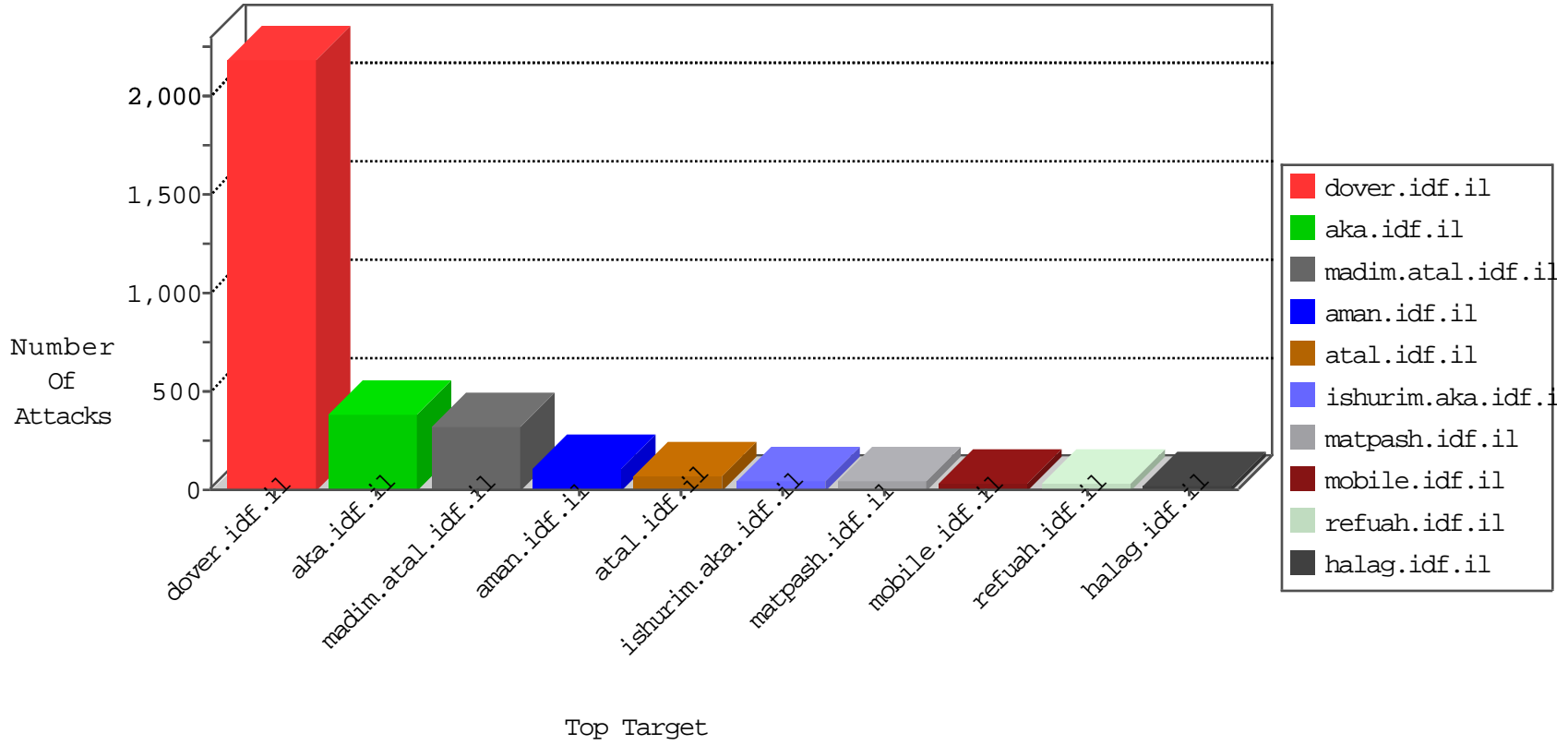


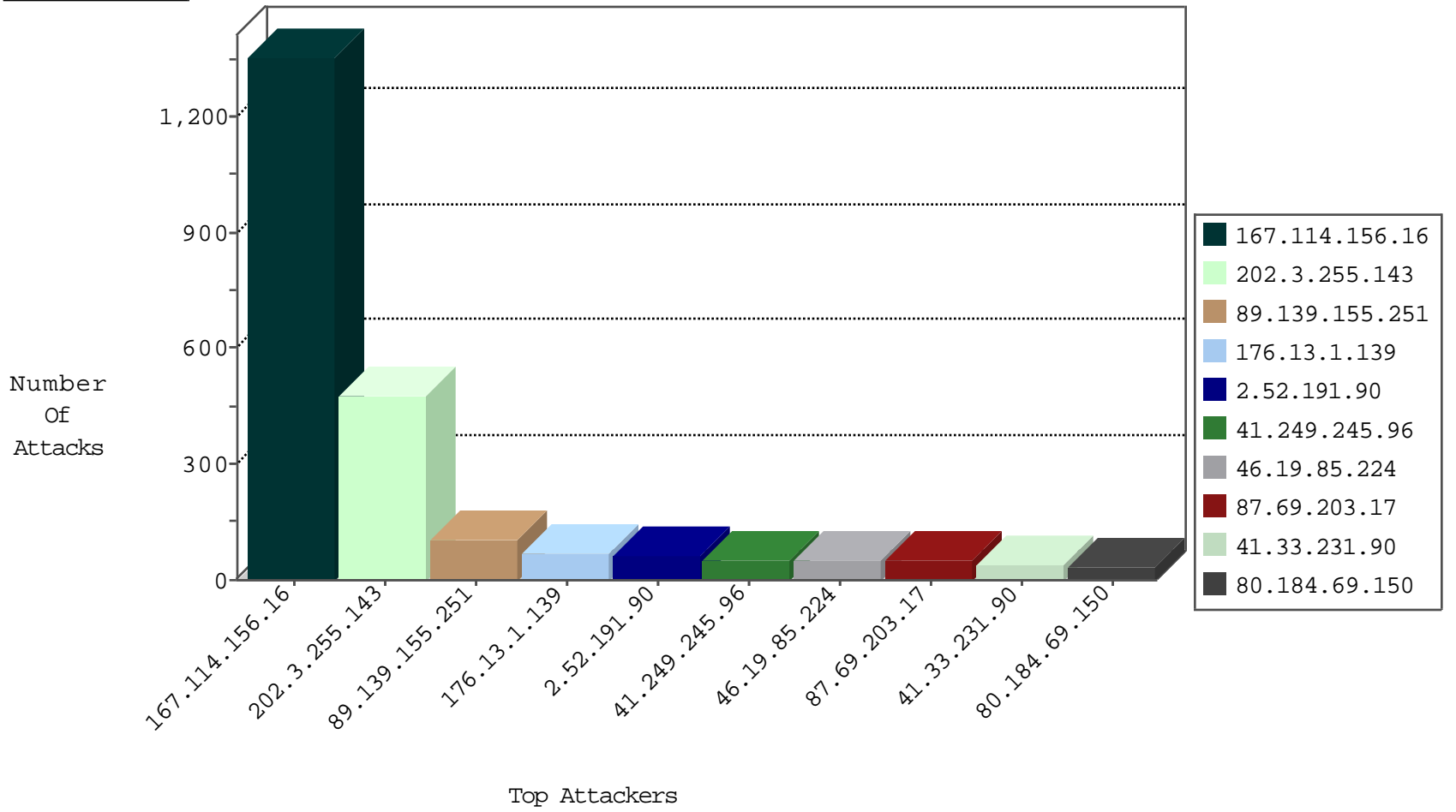
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3003
212.179.64.162	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
115.239.228.10	China	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Http	drop	2
203.98.87.42	Australia	147.237.76.39	mobile.meitav.idf.il	I4 Source or Dest Port Zero	drop	1
209.112.114.33	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid TCP Flags	drop	1
209.112.114.33	United States	147.237.77.227	e.hamaz.idf.il	Invalid TCP Flags	drop	1

01-17-2016-19:04:02 to 01-17-2016-20:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.143	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	437
41.249.245.96	147.237.77.216	Morocco	dover.idf.il	SERVER-WEBAPP awstats access	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	5
192.198.151.43	147.237.72.166	Europe	aka.idf.il	ET SCAN NMAP -sA (2)	2
41.249.245.96	147.237.77.216	Morocco	dover.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	2
41.249.245.96	147.237.77.216	Morocco	dover.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	2
84.109.1.119	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
79.181.4.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.157.212	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
191.240.136.5	147.237.76.44	Brazil	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
191.240.136.5	147.237.76.38	Brazil	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
45.32.64.164	147.237.76.42		refuah.idf.il	ET SCAN Potential SSH Scan	1
191.240.136.5	147.237.0.17	Brazil	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
45.32.64.164	147.237.0.35		akaws.idf.il	ET SCAN Potential SSH Scan	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
84.228.220.69	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.178.99	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.198	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.179.97	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
191.240.136.5	147.237.76.176	Brazil	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
191.240.136.5	147.237.76.39	Brazil	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
45.32.64.164	147.237.76.86		navy.idf.il	ET SCAN Potential SSH Scan	1
191.240.136.5	147.237.0.33	Brazil	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
45.32.64.164	147.237.76.30		himush.idf.il	ET SCAN Potential SSH Scan	1
183.82.106.200	147.237.0.17	India	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
105.154.211.228	147.237.77.216	Morocco	dover.idf.il	portscan: TCP Distributed Portscan	1
41.249.245.96	147.237.77.216	Morocco	dover.idf.il	POLICY-OTHER PHP uri tag injection attempt	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.52.191.90	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	51
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
41.249.245.96	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
80.184.69.150	Kuwait	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	31
46.19.85.139	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
79.183.221.148	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	18
37.26.147.188	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
79.183.133.68	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
166.216.165.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.52.191.90	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
95.35.167.35	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.142	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
5.22.134.220	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
80.246.140.143	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.183.234.200	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.86.10	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
188.120.148.231	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
5.29.117.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
5.22.135.231	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.218.55.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.178.212.92	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
213.8.204.30	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
82.137.166.102	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
84.228.220.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
58.11.8.43	Thailand	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.12	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.133.252	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.117.157.200	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.139.158	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.29.117.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
89.138.242.206	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.173	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.112	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
93.173.31.159	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
46.19.86.12	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.54.41.206	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
82.145.222.67	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
89.138.169.43	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.26.147.188	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	5
149.78.161.142	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.134.228	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.86.10	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.142.237.92	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.102.253.67	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.172	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.139.155.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
176.13.1.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	70
46.19.85.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
87.69.203.17	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 87.69.203.17	Block	49
80.246.136.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
2.52.190.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
87.69.195.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
89.139.155.251	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 89.139.155.251	Block	16
109.253.133.30	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
46.19.85.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.253.194.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
2.54.0.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
176.13.1.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.179.164.227	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00\$ContentPlaceHolder1\$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	3
109.253.157.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
149.78.6.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.127.158.82	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
80.246.140.143	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
104.238.117.86		147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	2
176.13.12.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.150.209.205	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=60800	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
176.13.15.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
187.45.193.166	Brazil	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	2
37.142.68.72	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
89.138.119.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/viewpayslip.aspx	Block	2
37.142.68.72	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	2
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1
200.73.116.212	Chile	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	1
5.22.134.220	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
87.118.64.36	Germany	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/wp-login.php	Block	1
176.13.3.188	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.232.178.12	Switzerland	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
198.1.70.245	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
84.111.233.43	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
172.93.122.57		147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
79.181.192.71	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
162.144.48.184	United States	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
46.19.85.179	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
92.63.140.212	United Kingdom	147.237.72.167	ishurim.aka.idf.il	Distributed PHP Attempt	Block	1
185.56.144.88	Netherlands	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
113.11.250.192	Singapore	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
212.48.81.89	United Kingdom	147.237.72.156	aman.idf.il	Distributed PHP Attempt	Block	1
5.255.253.62	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.138.185.33	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.18.238	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1