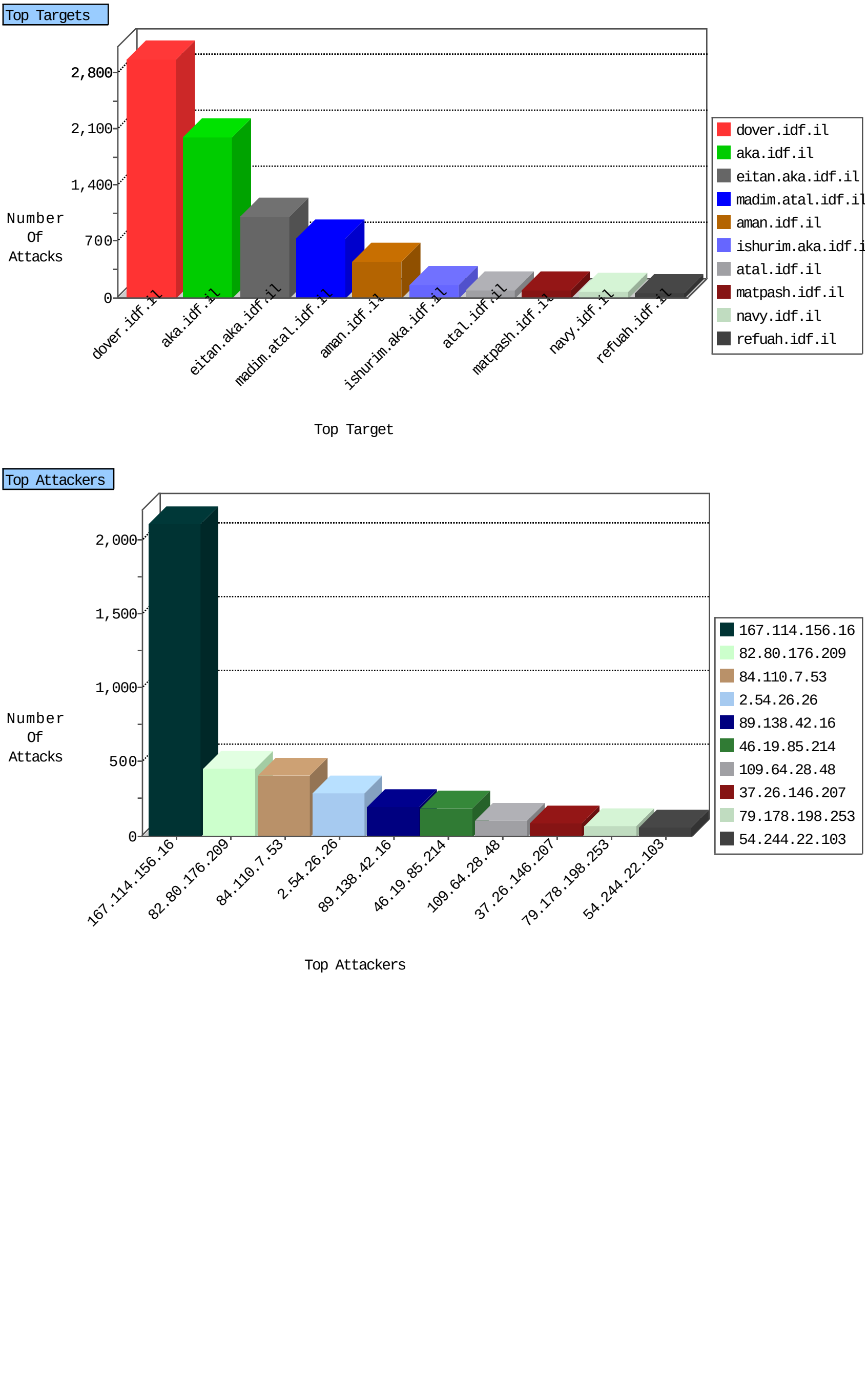
12-17-2015-15:04:06 to 12-17-2015-16:04:06

IDF Under Attack
Daily Report



12-17-2015-15:04:06 to 12-17-2015-16:04:06

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	3650
66.249.64.50	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	246
212.199.154.194	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	131
80.74.123.12	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
46.19.85.213	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
2.52.50.237	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
109.67.161.231	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
46.19.86.214	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
83.238.147.243	Poland	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.52.50.237	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
93.158.203.169	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
208.100.26.228	United States	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
79.183.128.21	Israel	147.237.72.166	aka.idf.il	Invalid L4 Header Length	drop	1
93.158.203.169	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1

12-17-2015-15:04:06 to 12-17-2015-16:04:06

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
62.210.90.118	France	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1

12-17-2015-15:04:06 to 12-17-2015-16:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
213.184.127.43	147.237.72.167	Israel	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	2
128.199.53.12	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
109.65.115.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.184.127.43	147.237.77.243	Israel	mobile.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
213.184.127.43	147.237.77.19	Israel	law-forum.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243	147.237.0.33		idf.il	ET SCAN NMAP -sS window 1024	1
213.184.127.43	147.237.76.148	Israel	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
213.8.204.61	147.237.77.216	Israel	dover.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
192.162.100.148	147.237.76.34	Russian Federation	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
149.50.74.227	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.174.109	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.159.206.102	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.184.127.43	147.237.77.226	Israel	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.113	147.237.0.16	Ukraine	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
213.184.127.43	147.237.76.196	Israel	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
212.143.148.178	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.196.7.170	147.237.77.216	Germany	dover.idf.il	portscan: TCP Distributed Portscan	1
166.63.125.149	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 4096	1

12-17-2015-15:04:06 to 12-17-2015-16:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
84.110.7.53	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	378
2.54.26.26	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	291
109.64.28.48	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	102
37.26.146.207	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	84
132.64.30.122	Israel	147.237.72.167	ishurim.aka.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	36
79.178.198.253	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	29
84.228.181.105	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	24
54.244.22.103	United States	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
84.110.7.53	Israel	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	23
207.241.229.104	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	23
79.178.198.253	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	22
2.54.53.121	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	22
46.19.86.48	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
176.13.1.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
79.180.170.89	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
77.125.152.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
84.108.219.119	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
84.108.219.119	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
109.67.161.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
62.219.192.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
2.54.137.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
62.219.192.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
89.138.42.16	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
37.142.190.206	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	16
31.168.20.73	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
62.219.192.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	16
37.26.146.141	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	15
46.117.252.23	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	15
2.54.19.249	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.54.137.175	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
80.246.136.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
176.12.141.191	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
80.246.136.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
37.142.190.206	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
46.121.246.20	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
46.120.69.191	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
46.121.246.20	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
54.244.22.103	United States	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
79.183.116.232	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
83.130.120.50	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	13
176.13.5.127	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
176.12.151.103	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	13
149.78.154.69	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
2.54.42.169	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
176.13.16.107	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
82.80.196.44	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
77.125.152.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	13
2.54.42.169	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13

12-17-2015-15:04:06 to 12-17-2015-16:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.176.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	231
89.138.42.16	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	184
82.80.176.209	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 82.80.176.209	Block	126
82.80.176.209	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
46.19.85.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	102
46.19.85.214	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	65
46.19.85.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
80.74.100.131	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	34
177.246.229.20	Mexico	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	13
84.110.7.53	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 84.110.7.53	Block	12
176.12.145.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
46.19.85.214	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtFirstName in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	6
176.13.10.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
2.54.19.249	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
103.252.17.160	Hong Kong	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	5
176.12.151.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
213.57.89.62	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22354-he/dover	Block	4
149.78.46.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
103.252.17.160	Hong Kong	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 103.252.17.160	Block	3
46.19.86.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.142.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
82.166.184.134	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 82.166.184.134	Block	3
176.12.148.183	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
142.4.215.116	Canada	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 142.4.215.116	Block	2
103.252.17.160	Hong Kong	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/plus/download.php	Block	2
91.143.80.201	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
176.13.13.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
82.166.184.134	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/5/size338x0/1565.jpg	Block	1
46.19.86.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
167.114.0.27	Canada	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/newsite/english/main.asp	Block	1
46.19.85.95	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
141.212.122.112	United States	147.237.76.31	nakchal.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
79.183.176.102	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.145	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/if/ad/2071700/0/300/250/square/nas%3aterastation	Block	1
5.29.117.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1153-he/dover.aspx	Block	1
185.32.179.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/recruitlane.aspx	Block	1
176.12.148.183	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
149.88.139.240	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
79.178.121.176	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
198.58.103.158	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
37.26.147.145	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.64.32.95	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
2.52.50.247	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
94.16.11.27	Germany	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.65.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/sa_swfobject.js	Block	1
84.109.194.23	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
176.12.139.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1

12-17-2015-15:04:06 to 12-17-2015-16:04:06