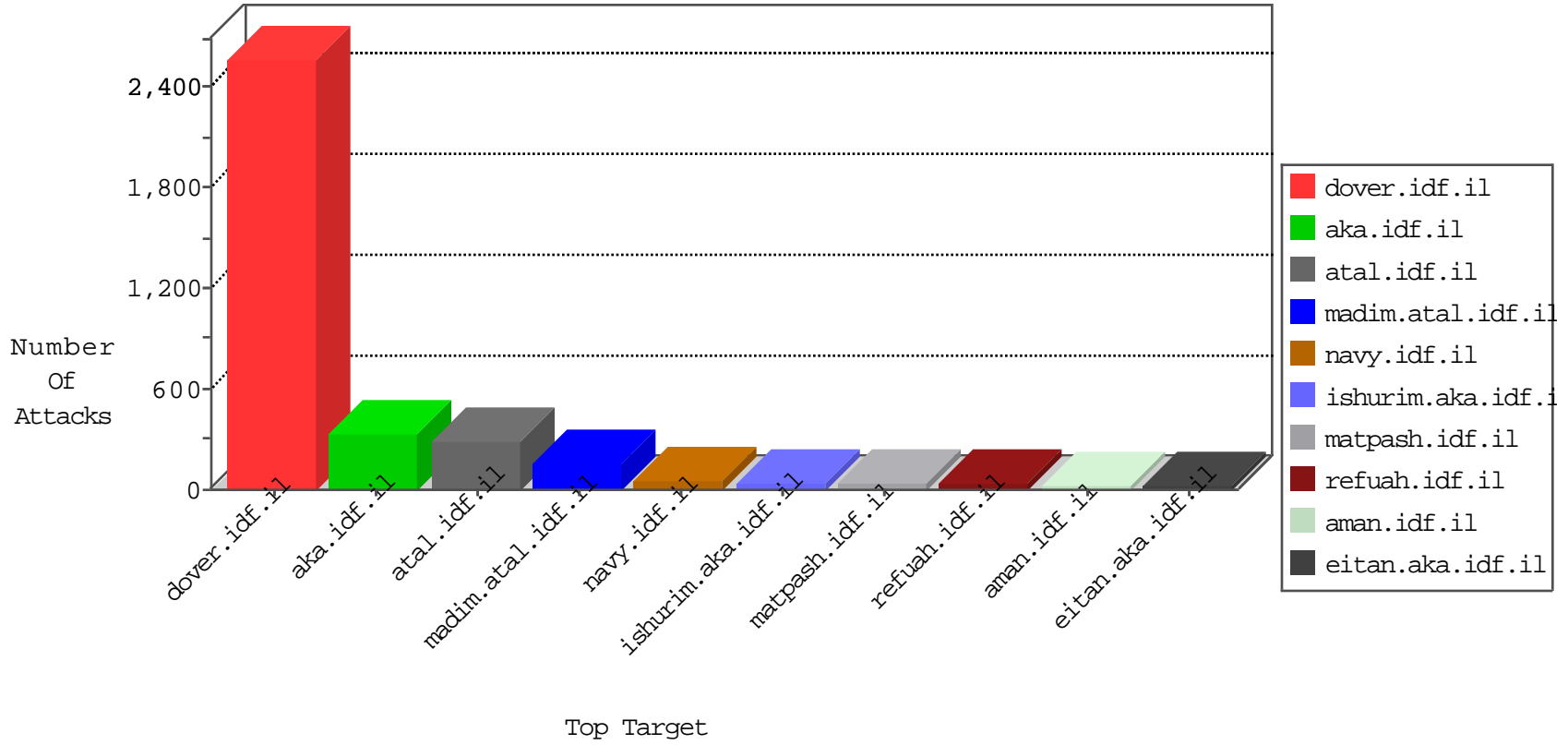


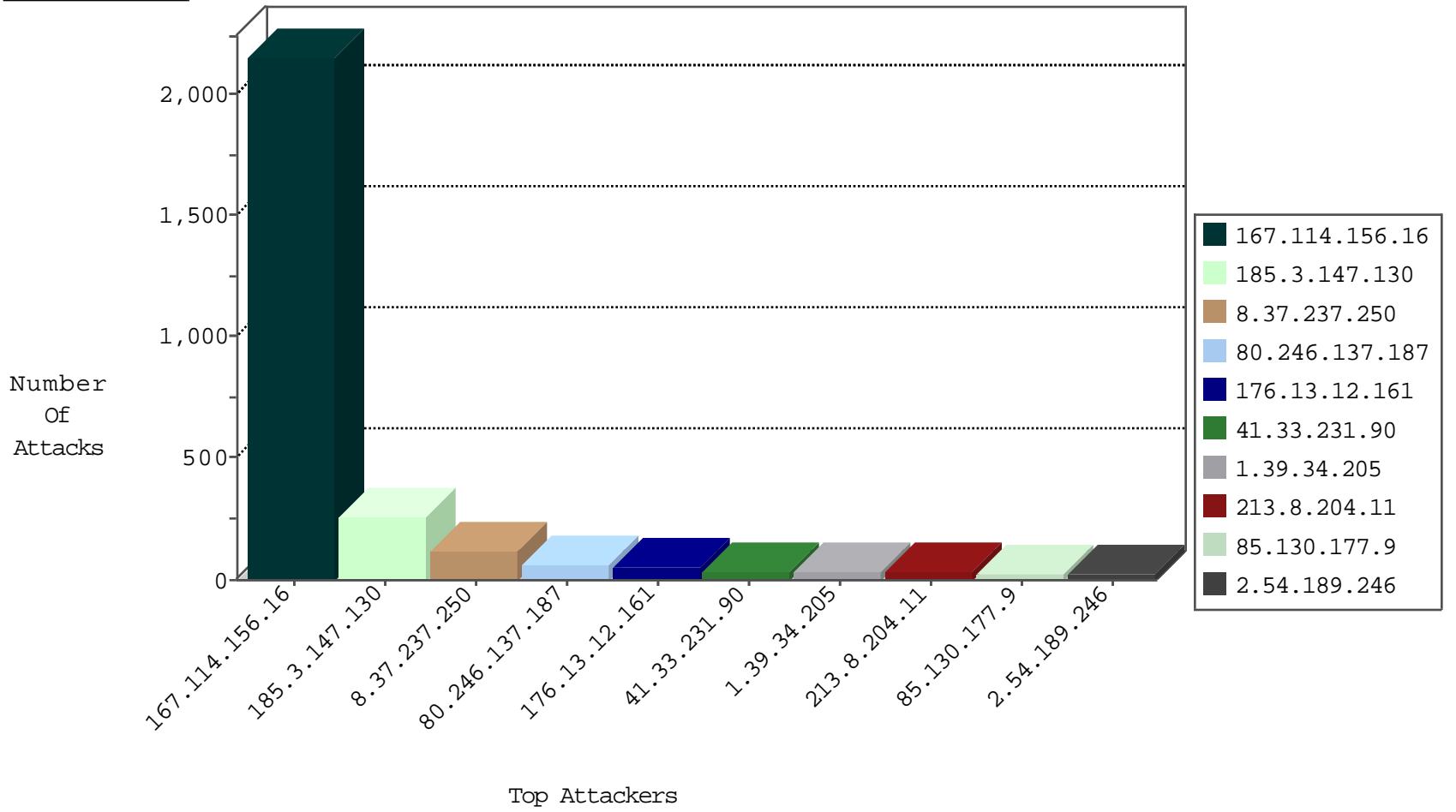
# IDF Under Attack Daily Report



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	3224
85.65.14.9	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
79.177.11.229	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
79.176.41.118	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
79.177.11.229	Israel	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	6
79.176.41.118	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
79.177.11.229	Israel	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	3
8.37.237.250	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
146.185.239.100	Russian Federation	147.237.76.147	chinuch.aka.idf.il	block-sp-trafl	drop	1
185.56.28.67	Netherlands	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
188.138.1.218	Germany	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
151.80.31.103	Italy	147.237.77.216	dover.idf.il	C228: HTTP: AhrefBot crawler	Block	1
37.187.137.225	France	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
122.112.77.58	China	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
149.78.139.175	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
113.171.23.126	147.237.0.16	Vietnam	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
109.65.141.168	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.231.193.150	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.166.20.64	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.155.91	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
121.201.27.61	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
109.66.103.252	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
95.86.80.141	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.68.150.129	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.144.170.190	147.237.76.34	United Kingdom	yohalan.idf.il	ET SCAN NMAP -sS window 3072	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.3.147.130	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	248
8.37.237.250	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	119
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
1.39.34.205	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
84.94.43.81	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
109.186.99.117	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
37.142.68.103	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
2.54.189.246	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
176.13.7.54	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
176.13.7.54	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
149.78.167.172	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
79.179.155.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
185.3.147.130	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
85.130.177.9	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
80.178.213.67	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.85.11	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
85.65.14.9	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.168.17.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.11	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.235.83.154	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
1.39.34.205	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.11	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
79.179.131.237	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	alert	6
46.19.85.11	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
66.249.64.188	United States	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
85.65.14.9	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.179.131.237	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.179.214.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.115.83.5	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.153	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.102.253.5	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.181.139.62	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
188.120.148.188	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
1.39.34.205	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
31.210.188.104	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.189.246	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
2.54.11.16	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.189.246	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.66.103.70	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.54.13.38	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.189.246	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
2.52.34.62	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
31.210.188.59	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.183.128	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.137.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	65
176.13.12.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
213.8.204.11	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 213.8.204.11	Block	32
80.246.136.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
183.79.221.239	Japan	147.237.76.200	eitan.aka.idf.il	Multiple Abnormally Long Request from 183.79.221.239	Block	8
183.79.221.239	Japan	147.237.76.200	eitan.aka.idf.il	Multiple Illegal HTTP Version from 183.79.221.239	Block	8
80.246.136.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
17.138.57.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-he	Block	4
80.246.136.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
213.57.141.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
95.86.107.124	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatgauntity.aspx	Block	2
84.94.38.200	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/authenticationsevice.asmx/getauthuser	Block	2
149.88.53.149	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	2
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	2
17.138.57.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22248-he/dover.aspx	Block	2
2.52.4.33	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
80.246.136.143	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
89.31.57.5	Italy	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.75.116	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 5cf35968 in aka.idf.il/news/	None	1
184.168.200.168	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
37.26.146.190	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/layout.css	Block	1
176.13.9.135	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
2.52.37.29	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.138.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.179.214.222	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/valtam	Block	1
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	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	1
50.62.176.42	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
183.79.221.239	Japan	147.237.76.200	eitan.aka.idf.il	Illegal HTTP Version *?x*x*x*x" HTTP/1.0	Block	1
85.65.166.152	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/	Block	1
5.102.253.41	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://www.idf.il/	Block	1
149.78.166.151	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.176.124.71	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in www.atal.idf.il/1440-he/atal.aspx	Block	1
109.66.139.201	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.138.168.25	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
185.3.147.130	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
37.26.146.246	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.40.146	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.218.105	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.181.130.132	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct166.x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
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	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
50.62.176.42	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
85.65.233.61	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.178.142.206	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.67.228.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1