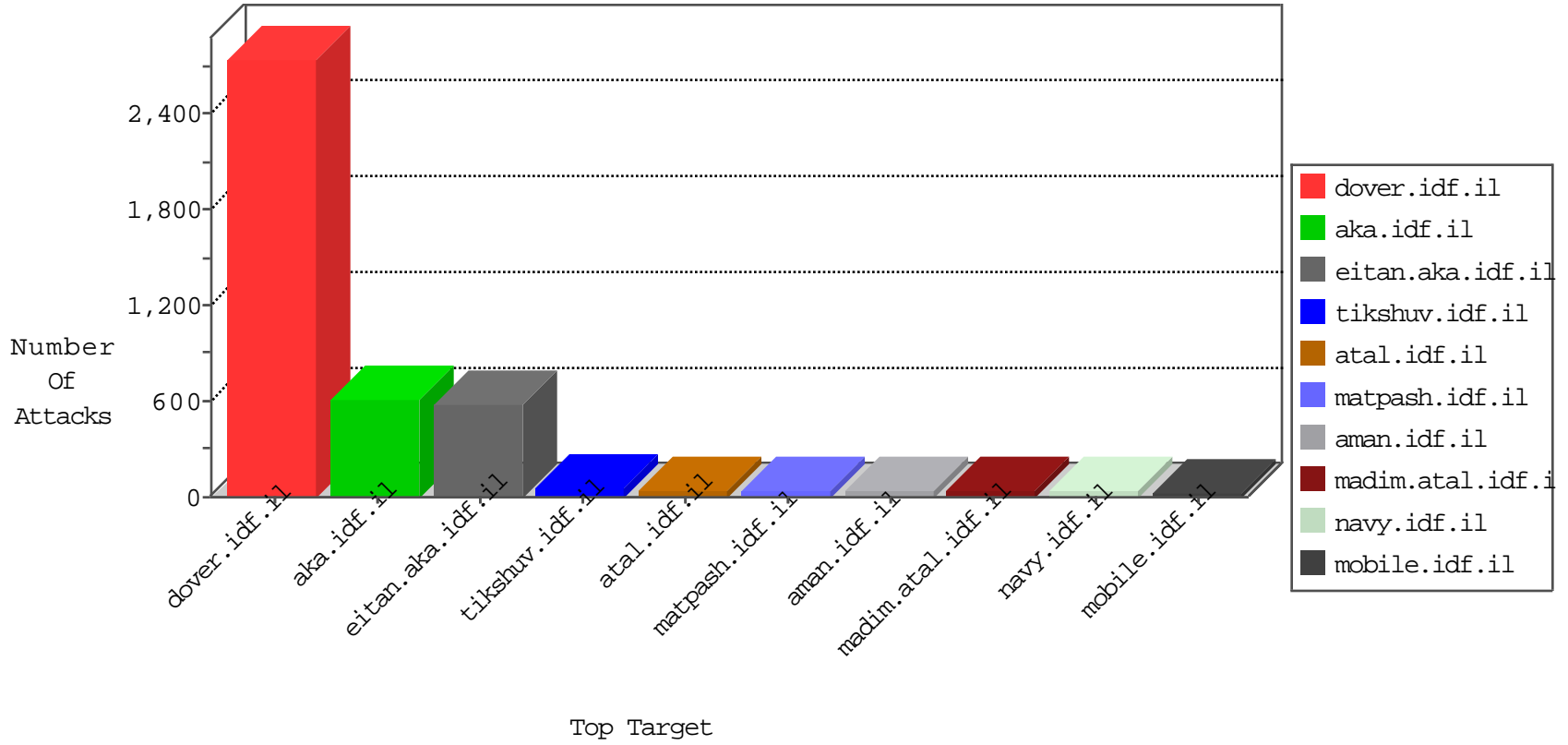


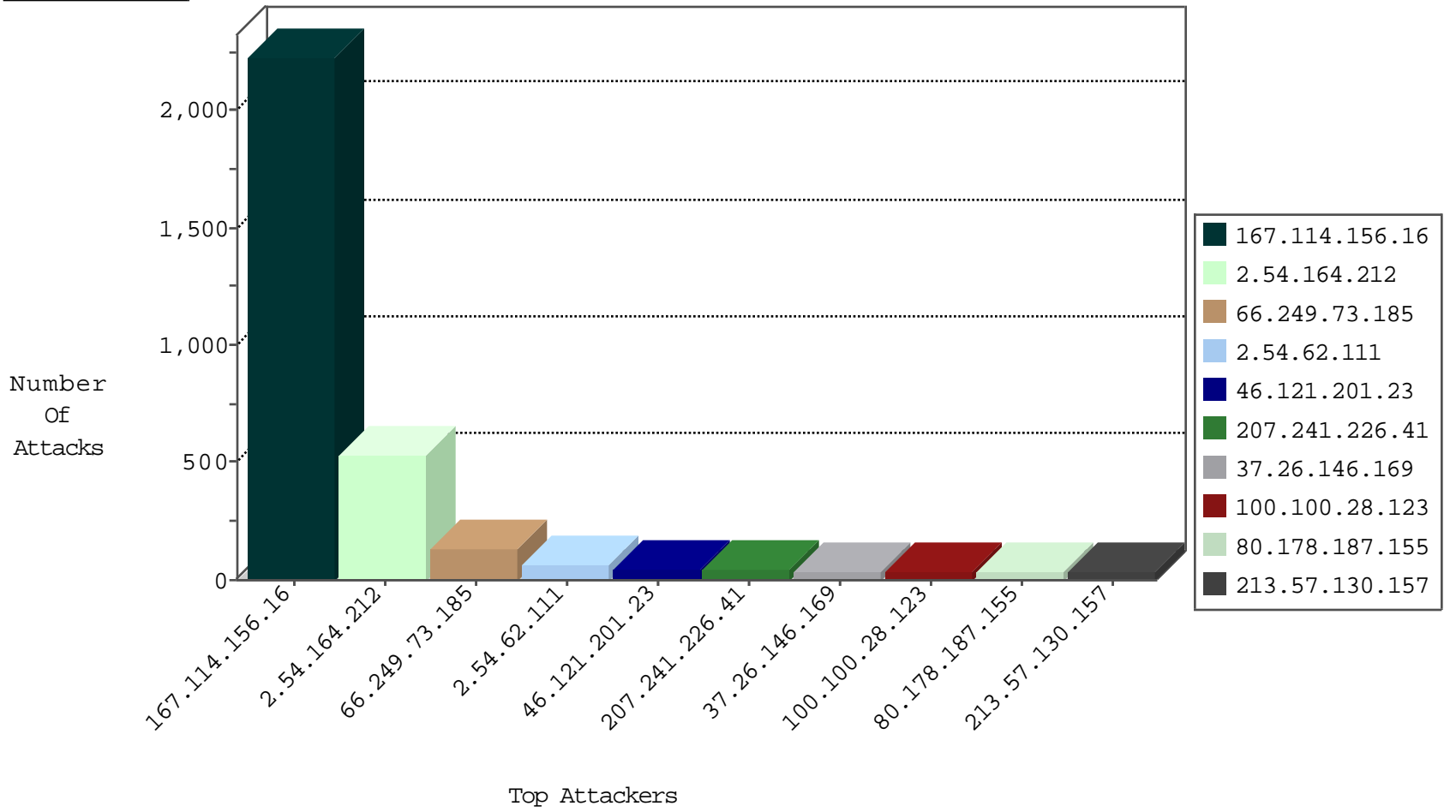
# IDF Under Attack Daily Report



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	3592
66.249.66.125	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	22
84.108.235.46	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	4
84.108.235.46	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
119.10.1.42	China	147.237.76.199	e.nakchal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
63.143.34.37	United States	147.237.77.233	atal.idf.i	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	8
24.47.146.194	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
24.47.146.194	United States	147.237.77.74	law.idf.il	3809: HTTP: SQL Injection Evasion SQL Comment Terminator	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
63.143.34.37	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	24
24.47.146.194	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	7
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
111.49.145.192	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	2
79.178.188.111	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
111.49.145.192	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
111.49.145.192	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
37.26.146.198	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
111.49.145.192	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
31.6.71.154	147.237.77.205	Poland	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
111.49.145.192	147.237.76.177	China	noore.idf.il	ET SCAN Potential SSH Scan	1
2.54.63.87	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
111.49.145.192	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
222.78.0.176	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
111.49.145.192	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
197.157.244.243	147.237.77.216	Somalia	dover.idf.il	ET SCAN Potential SSH Scan	1
111.49.145.192	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
100.13.108.185	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
185.56.80.31	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.73.185	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
111.49.145.192	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
37.26.149.248	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
111.49.145.192	147.237.77.170	China	maarachot.idf.il	ET SCAN Potential SSH Scan	1
31.154.88.158	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
111.49.145.192	147.237.76.148	China	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
111.49.145.192	147.237.76.34	China	yochalan.idf.il	ET SCAN Potential SSH Scan	1
208.80.155.223	147.237.76.86	United States	navy.idf.il	Tehila - Perl LWP with fake user agent	1
111.49.145.192	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
197.157.244.243	147.237.72.166	Somalia	aka.idf.il	ET SCAN Potential SSH Scan	1
111.49.145.192	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
185.56.80.31	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.164.212	Israel	147.237.76.200	eitan.aka.idf..	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	477
66.249.73.185	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	134
46.121.201.23	Israel	147.237.76.200	eitan.aka.idf..	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
37.26.146.169	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	39
213.57.130.157	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
66.249.73.193	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
2.54.62.111	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
107.72.162.111	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	24
100.100.116.202		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	24
100.100.28.123		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	22
31.154.91.4	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	21
213.57.128.172	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	21
80.178.187.155	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
80.178.187.155	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	17
213.57.131.178	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	16
100.100.29.63		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
100.100.57.60		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
100.100.28.123		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
66.249.81.218	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
5.22.134.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
213.57.131.178	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
149.88.30.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.25.97		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
66.102.9.54	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	11
213.57.143.232	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
100.100.107.242		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
2.54.62.111	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
37.26.149.199	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
100.100.124.9		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
2.54.62.111	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
213.57.128.231	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
2.54.62.111	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
46.19.85.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
176.228.175.128	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.85.90	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.65.172.149	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
66.249.81.212	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
185.32.179.201	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.86.70	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
2.52.132.166	Israel	147.237.76.86	navy.idf.il	SYN Attack		reject	7
2.54.153.32	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.228.7.49	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.30	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.184.52	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.30	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
24.179.11.167	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.164.212	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	55
207.241.226.41	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 207.241.226.41	Block	39
212.76.103.16	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	9
5.102.247.156	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	6
85.64.150.174	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	5
46.19.85.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.228.175.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
207.241.226.41	United States	147.237.0.34	tikshuv.idf.il	PHP Attempt	Block	3
176.13.19.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
31.154.92.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.168.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.65.172.149	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.180.211.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	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
46.19.85.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
46.19.86.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
207.46.13.99	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
89.139.165.104	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.85.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.178.187.155	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.228.175.128	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.176.110.252	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
109.65.137.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.176.127.80	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/	Block	2
46.19.85.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.65.3.119	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx parameter	None	1
66.249.66.65	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/320/patzar.aspx	Block	1
82.81.4.254	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/	Block	1
46.121.201.23	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized Method POST for www.eitan.aka.idf.il/1099-he/eitan.aspx	None	1
149.78.138.106	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/main/home/default.aspx	Block	1
212.143.23.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/	Block	1
37.142.64.101	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
87.69.190.81	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.13.3.83	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method	Block	1
5.29.92.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	1
84.228.27.76	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.244	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.186.173.161	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/chinuch/klali/	None	1
80.86.94.7	Germany	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 80.86.94.7	Block	1
79.178.202.64	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/ufi/reaction/	Block	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
31.154.92.26	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
85.65.43.105	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
66.249.69.81	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1275-he/atal.aspx	Block	1
176.228.7.49	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.22.134.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1