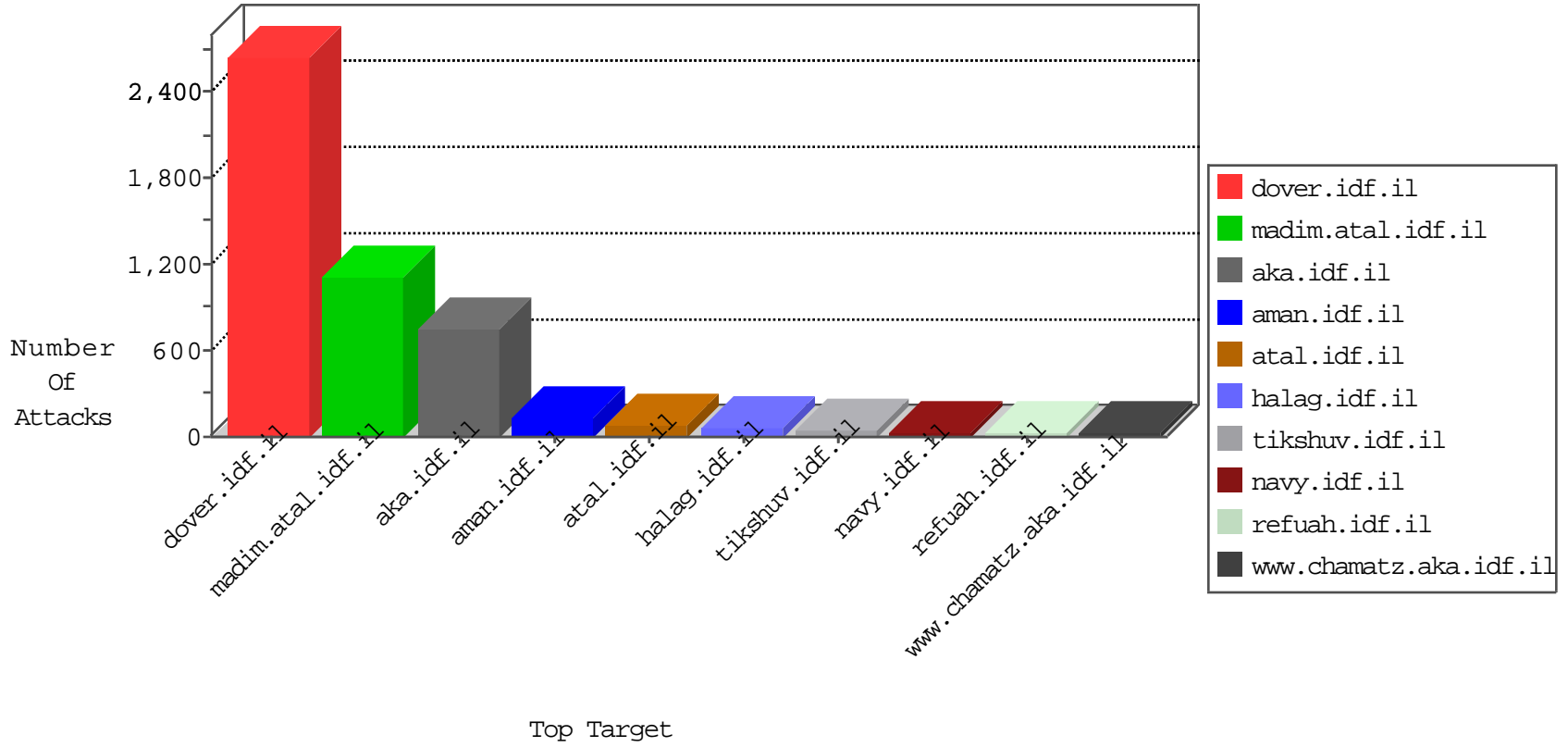


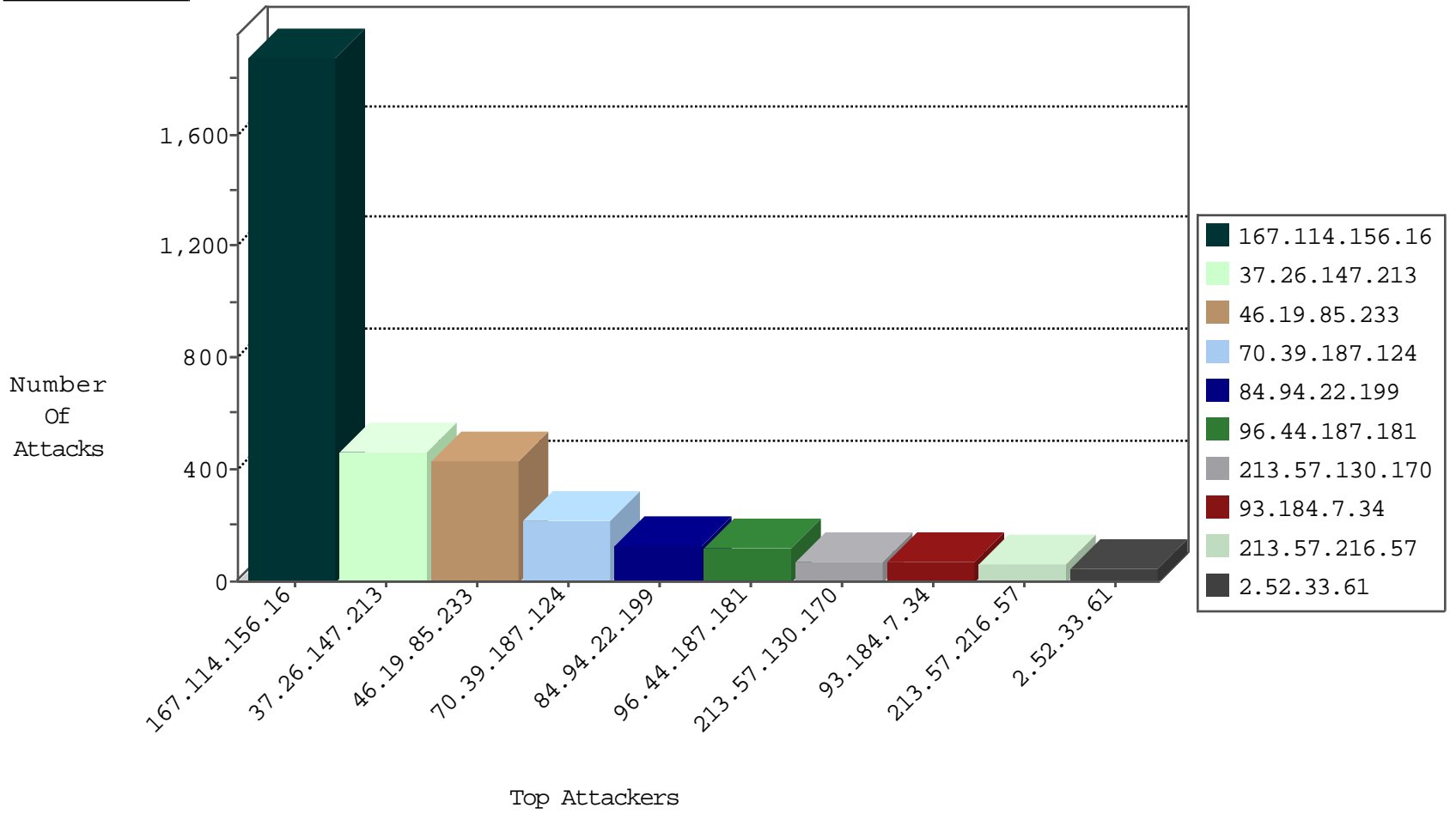
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.254	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	12029
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3153
212.29.246.85	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	18
46.19.86.69	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	11
146.185.57.7	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
96.44.187.181	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
70.39.187.124	Satellite Provider	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
188.119.26.176	Turkey	147.237.76.34	ychalan.idf.il	Block_Udp_All_Nets	drop	1
157.161.177.76	Switzerland	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
2.93.241.251	Russian Federation	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
188.119.26.176	Turkey	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
70.39.187.124	Satellite Provider	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
188.119.26.176	Turkey	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
96.44.187.181	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	36
96.44.187.181	United States	147.237.77.216	dover.idf.il	0854: HTTP: upload* Access	Block	11
62.0.54.2	Israel	147.237.77.170	maarachot.idf.il	C1000122: HTTP: Access to - .exe or .dll	Permit	1
96.44.187.181	United States	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	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	4
66.249.93.15	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
37.26.147.213	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
81.218.101.3	147.237.77.216	Israel	dover.idf.il	http_inspect: MULTIPLE HOST HEADERS DETECTED	1
137.116.113.55	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential SSH Scan	1
137.116.113.55	147.237.76.148	United States	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
137.116.113.55	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
2.52.33.61	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
137.116.113.55	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential SSH Scan	1
222.186.42.207	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
109.66.106.110	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.57	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.172.233	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
186.14.185.223	147.237.76.30	Venezuela	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
93.173.159.205	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.2.110	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.150.246	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
137.116.113.55	147.237.76.202	United States	e.halag.idf.il	ET SCAN Potential SSH Scan	1
79.181.211.21	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
137.116.113.55	147.237.76.177	United States	ncore.idf.il	ET SCAN Potential SSH Scan	1
62.0.54.2	147.237.77.170	Israel	maarachot.idf.il	WEB-FRONTPAGE /_vti_bin/ access	1
137.116.113.55	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
31.210.179.53	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
137.116.113.55	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
137.116.113.55	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
213.57.180.74	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.110.24	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.208	147.237.76.44		e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
84.109.215.128	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
143.176.244.40	147.237.77.216	Netherlands	dover.idf.il	portscan: TCP Distributed Portscan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
70.39.187.124	Satellite Provider	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	120
70.39.187.124	Satellite Provider	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	96
93.184.7.34	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	SAM rule	drop	64
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
96.44.187.181	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	30
213.57.130.170	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	22
213.57.130.170	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	22
213.57.130.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	22
80.246.137.188	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
46.19.85.86	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
46.19.86.116	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
5.102.197.244	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
79.181.97.188	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
77.126.15.125	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
46.19.86.92	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
84.228.88.187	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
176.228.7.49	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
109.253.145.52	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
176.228.7.49	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
37.46.39.73	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.86.223	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.86.151	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
87.68.37.221	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
84.228.59.49	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
2.52.33.61	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.52.33.61	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	8
2.52.33.61	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
2.52.33.61	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.52.33.61	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
46.19.86.223	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
84.228.56.112	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.15	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
87.69.32.107	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.25.10	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.67.127.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.117.66.51	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.117.66.51	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.178.150.219	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.133	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.125.144.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.179.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.53.87	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.119	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.69.32.107	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.93.123	United States	147.237.77.233	atal.idf.il	drop		drop	6
212.29.246.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.147.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	246
46.19.85.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	205
46.19.85.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	153
37.26.147.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	147
84.94.22.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	90
46.19.85.233	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.233	Block	65
213.57.216.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
37.26.147.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	49
84.94.22.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	40
96.44.187.181	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 96.44.187.181	Block	29
80.246.130.92	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 80.246.130.92	Block	17
37.26.147.213	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 37.26.147.213	Block	14
109.253.204.180	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation ctl00\$ContentPlaceHolder1\$txtAreaRemarks in m.my-kosher-kravi.idf.il/templates/training/training.aspx	Block	8
46.19.85.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	6
109.67.4.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
149.88.252.34	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
192.116.159.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.15.123	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
96.44.187.181	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
87.69.67.209	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/general.aspx	Block	2
80.246.130.92	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/	Block	2
31.210.187.152	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.253.130.152	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.183.153.107	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
149.78.161.202	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
31.154.9.62	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
77.126.61.12	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
84.228.54.84	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
80.246.130.92	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catld in www.aka.idf.il/main/giyus/general.aspx	None	2
176.13.12.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.179.5.232	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.58	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/1133-22461-he/dover.aspx.	Block	2
217.132.34.56	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	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
46.121.213.94	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.228.219.189	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.13.12.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.182.53.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.65.25.31	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.29.164.176	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.179.30.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.57.189.19	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
46.19.86.204	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.108.184.84	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.23.66	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
72.46.133.242	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
192.114.5.10	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
46.19.85.112	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1