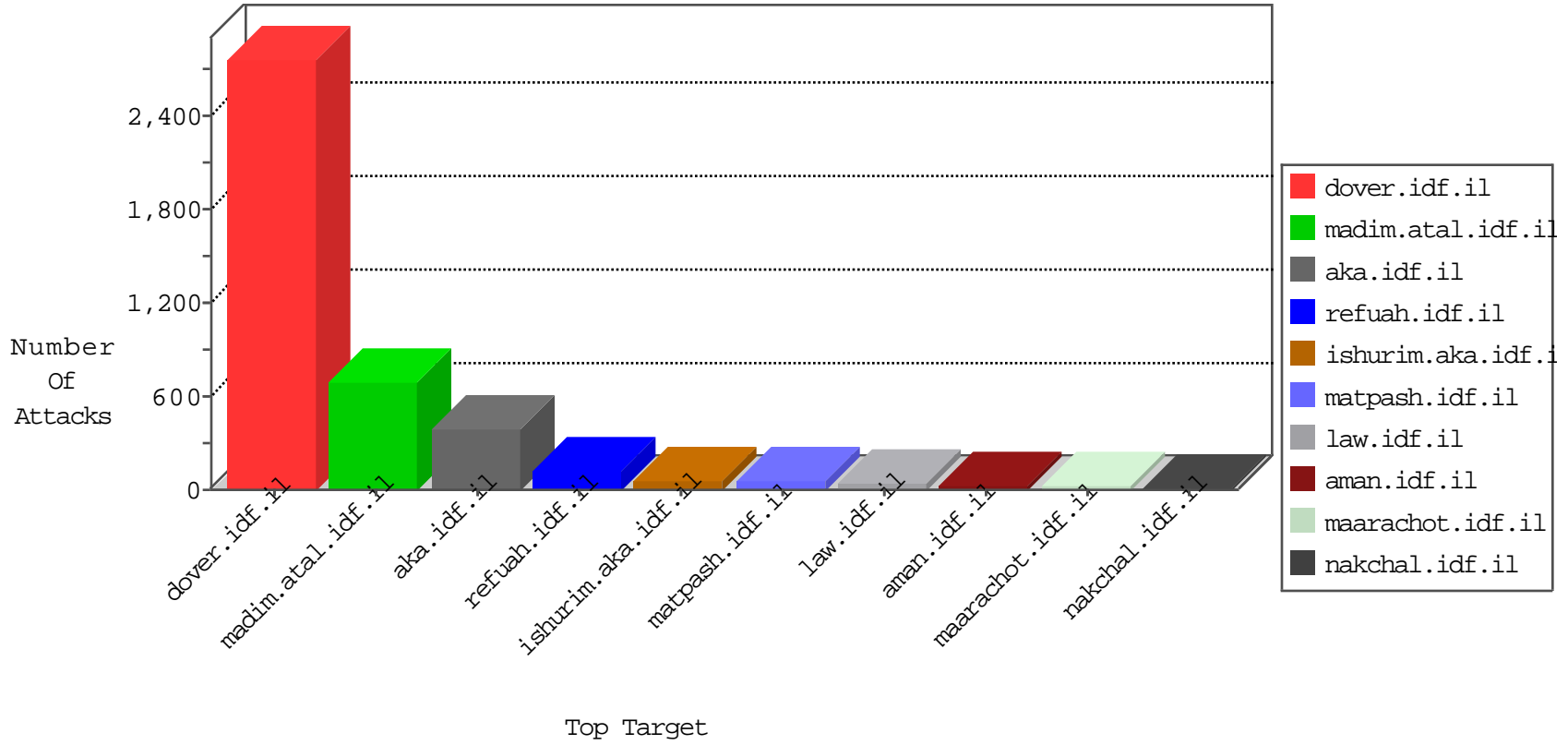


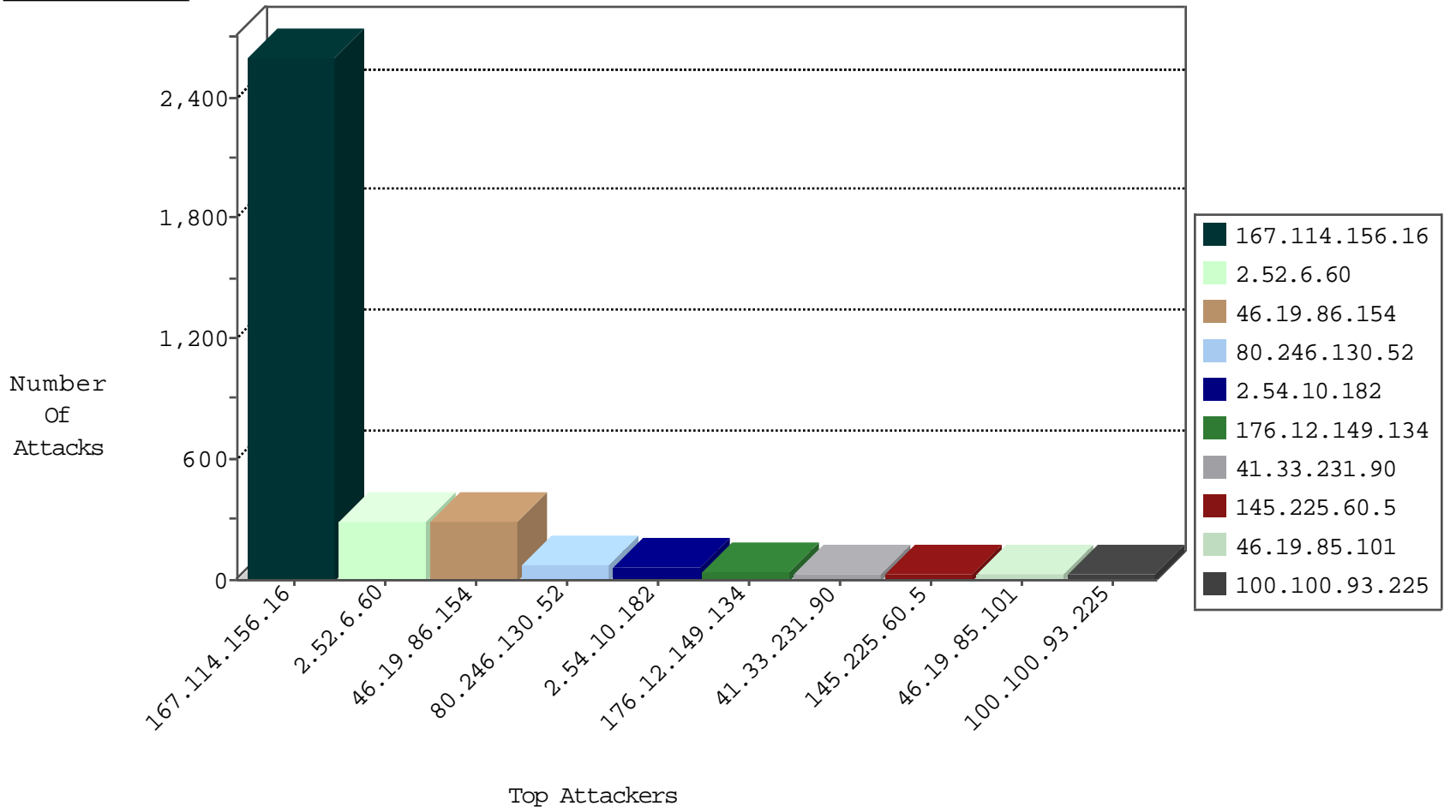
# IDF Under Attack Daily Report



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	3534
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	104
180.97.106.162	China	147.237.0.15	kosher-kravi.idf.il	block-sp-trafl	drop	1
94.158.39.128	Ukraine	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
180.97.106.36	China	147.237.77.216	dover.idf.il	block-sp-trafl	drop	1
180.97.106.37	China	147.237.76.200	eitan.aka.idf.il	block-sp-trafl	drop	1
37.26.148.170	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
180.97.106.36	China	147.237.72.166	aka.idf.il	block-sp-trafl	drop	1
180.97.106.37	China	147.237.77.74	law.idf.il	block-sp-trafl	drop	1
180.97.106.36	China	147.237.76.31	nakchal.idf.il	block-sp-trafl	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.247.122.28	Spain	147.237.77.176	matpash.idf.il	13248: HTTP: Joomla JCE File Upload Remote Code Execution Vulnerability	Block	2
162.210.196.97	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
195.154.211.20	France	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
77.127.25.97	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.108.132.58	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.71	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.62.18.235	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.226	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.112.102.211	147.237.8.50		e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
5.102.228.18	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
173.160.184.241	147.237.76.148	United States	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 2048	1
2.54.132.67	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
132.70.66.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
82.117.208.243	147.237.8.46		e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
80.178.148.49	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.108.132.58	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.79.133	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sA (2)	1
195.154.194.59	147.237.77.216	France	dover.idf.il	LOCAL_RULES - Request with the string install.php in it	1
37.247.122.28	147.237.77.176	Spain	matpash.idf.il	Tehila - Perl LWP with fake user agent	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
37.26.148.170	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	1
185.110.157.13	147.237.0.35		akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
2.54.190.35	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
173.160.184.241	147.237.76.148	United States	ggcenter.aka.idf.il	ET SCAN NMAP -f -sS	1
128.139.19.191	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.130.248.8	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.246.130.52	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	73
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
145.225.60.5	Germany	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	30
46.19.85.101	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
100.100.93.225		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
193.17.232.2	Germany	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	20
80.246.138.208	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
37.26.148.227	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
87.69.80.137	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
46.19.86.154	Israel	147.237.0.19	madim.atal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
82.80.52.65	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
36.48.69.131	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
37.26.146.139	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.180.51.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.148.175	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.86.49	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
36.48.69.131	China	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
173.252.75.115	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
87.69.80.137	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
188.120.148.174	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.58.75	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
147.236.238.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.118.27.253	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.52.53.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.201	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.152	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.52.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
100.100.93.225		147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	6
194.90.66.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.34.81.220	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
36.48.69.131	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.181.214.21	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.57.132.7	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
85.130.177.9	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.31	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
62.0.34.177	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
212.179.21.194	Israel	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.73	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.154	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
109.67.125.144	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.154	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.31	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
213.57.143.74	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.154	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
213.57.132.7	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
207.46.13.176	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.130.223.241	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.178.113.38	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	130
2.52.6.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	122
46.19.86.154	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.154	Block	110
2.52.6.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
2.54.10.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	67
2.52.6.60	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 2.52.6.60	Block	66
176.12.149.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
46.19.86.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	29
194.90.134.226	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	9
31.154.166.57	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/	Block	6
2.86.60.213	Greece	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	4
2.86.60.213	Greece	147.237.76.42	refuah.idf.il	PHP Attempt	Block	4
212.143.186.38	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.143.186.38	Block	3
176.12.139.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.130.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
194.90.134.226	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	3
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	3
31.154.166.57	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	3
185.32.179.199	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.20.106	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.56.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
91.200.12.139	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
66.249.93.254	Israel	147.237.76.42	refuah.idf.il	Distributed Parameter Type Violation on www.refua.atal.idf.il/1518-he/refuah.aspx parameter ct100\$ContentPlaceholder1\$txtContent	Block	2
212.143.3.44	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
66.249.64.243	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
2.54.31.190	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
82.166.159.63	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.228	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 46.19.86.228	Block	1
79.183.144.86	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
46.19.85.34	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.9.162	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
128.232.110.29	United Kingdom	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
68.180.228.109	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation PageNum in www.tikshuv.idf.il/901-he/tikshuv.aspx	Block	1
93.172.147.233	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
65.78.117.21	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/rights/asp/info.asp	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
176.13.17.229	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.130.52	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
79.177.24.70	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
217.194.203.76	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
37.26.149.243	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.247	United States	147.237.77.233	atal.idf.il	Abnormally Long Request URL	Block	1
66.249.66.64	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-22461-he/dover.aspx.	Block	1
2.52.31.60	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.94.41.76	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.120.18.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1