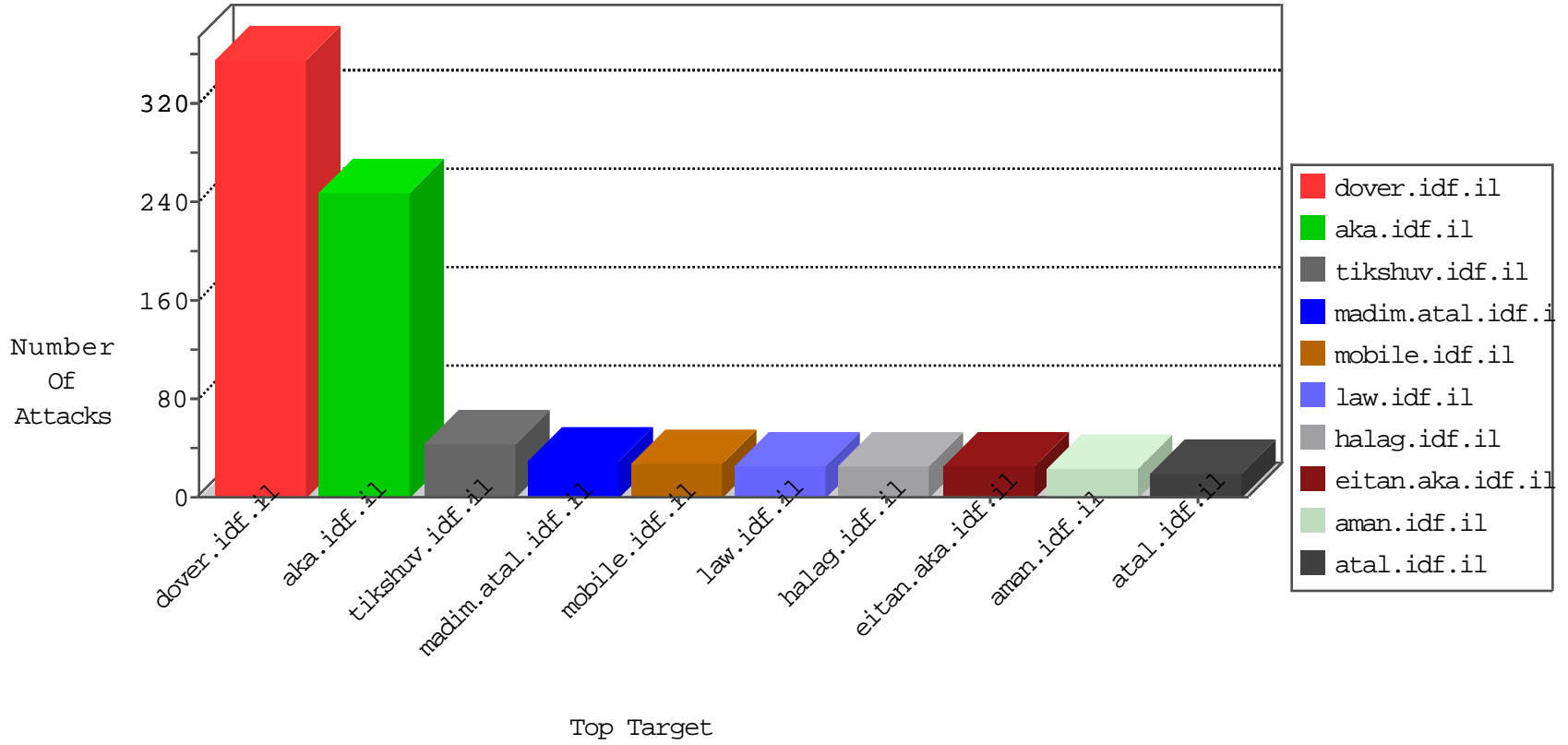


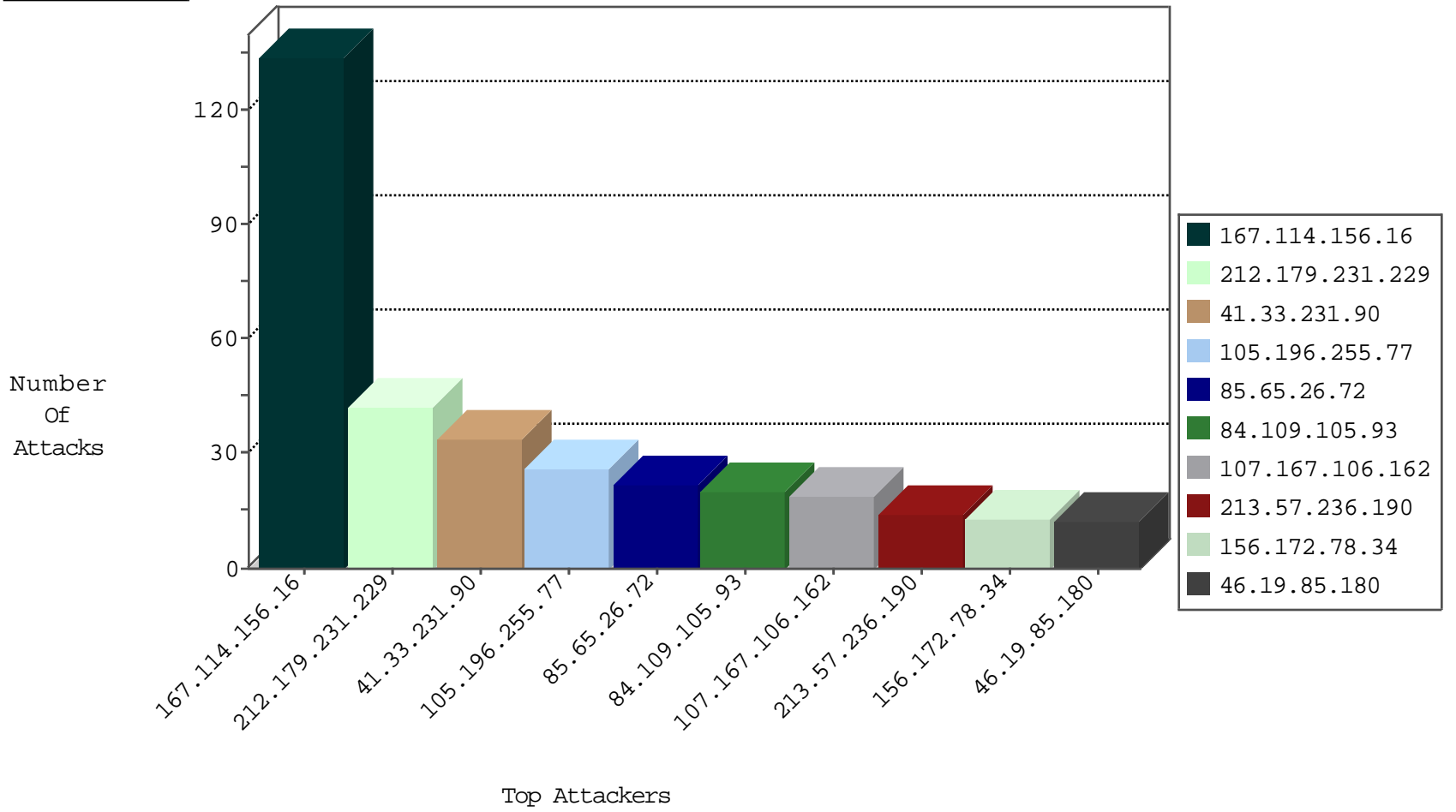
IDF Under Attack Daily Report



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	3071
66.249.78.254	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	906
167.114.156.16	Canada	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	6
185.130.5.224		147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.122	Netherlands	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
142.54.160.213	United States	147.237.77.233	atal.idf.il	block-sp-traf1	drop	1
207.46.13.158	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
107.150.60.78	United States	147.237.77.74	law.idf.il	block-sp-traf1	drop	1
89.248.174.4	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
107.150.60.244	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	drop	1
94.102.49.122	Netherlands	147.237.76.148	ggcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
142.54.160.211	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	drop	1

01-09-2016-15:04:00 to 01-09-2016-16:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.66	France	147.237.72.156	aman.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.75	France	147.237.77.234	halag.idf.il	C228: HTTP: AhrefBot crawler	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
64.251.164.129	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN Potential SSH Scan	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
59.45.79.117	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
80.200.14.144	147.237.0.19	Belgium	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
78.193.2.8	147.237.0.19	France	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
64.251.164.129	147.237.77.243	United States	mobile.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
201.235.215.254	147.237.76.202	Argentina	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
199.191.56.188	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 3072	1
59.45.79.117	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
64.251.164.129	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
187.160.86.53	147.237.76.34	Mexico	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
64.251.164.129	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
123.203.80.154	147.237.76.30	Hong Kong	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
64.251.164.129	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
107.191.63.157	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
80.200.14.144	147.237.0.34	Belgium	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
79.176.112.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
78.193.2.8	147.237.0.15	France	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
201.235.215.254	147.237.76.202	Argentina	e.halag.idf.il	ET SCAN NMAP -sS window 4096	1
64.251.164.129	147.237.77.233	United States	atal.idf.il	ET SCAN Potential SSH Scan	1
201.235.215.254	147.237.76.202	Argentina	e.halag.idf.il	ET SCAN NMAP -f -sS	1
59.45.79.117	147.237.72.217	China	e.idf.il	ET SCAN Potential SSH Scan	1
64.251.164.129	147.237.77.212	United States	e.dover.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
64.251.164.129	147.237.72.156	United States	aman.idf.il	ET SCAN Potential SSH Scan	1
158.255.2.52	147.237.72.167	Russian Federation	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
64.251.164.129	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
107.191.63.157	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
107.191.63.157	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.231.229	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
85.65.26.72	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
105.196.255.77	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
105.196.255.77	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
77.127.217.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.120.114.67	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
81.218.167.179	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
156.172.78.34		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	9
109.160.247.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
84.109.105.93	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
79.182.137.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.45	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.188.56	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
213.57.236.190	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
31.210.188.41	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.109.105.93	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.216.172.74	Belarus	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
41.35.15.176	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.210.182	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.64.146.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.187	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
85.64.216.20	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
66.249.66.90	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.142.236.192	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
5.102.254.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.11	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
109.253.205.22	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
84.109.105.93	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
85.65.61.146	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
213.57.236.190	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
94.230.86.179	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.182.216.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.180.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
70.194.211.71	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
2.54.147.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
128.127.107.108	Netherlands	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
24.114.92.186	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
94.159.169.138	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.153.104	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.172.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.116	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.28.129.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
5.29.76.120	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/giyus/authentication-service.aspx/getauthuser	Block	6
192.243.55.129	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.129	Block	4
176.13.20.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
188.143.232.21	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.21	Block	3
94.159.169.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.29.60.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.243.55.138	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.138	Block	3
5.22.130.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	2
31.210.179.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
207.46.13.158	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.158	Block	2
50.62.161.195	United States	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
77.126.166.234	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	2
79.181.55.225	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.186.189.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.94.38.200	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authentication-service.aspx/getauthuser	Block	2
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
37.142.236.192	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
50.62.176.169	United States	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
213.57.224.10	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1232-he/atal.aspx	Block	1
89.219.120.12	Estonia	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/giyus/main/default.asp	Block	1
50.62.161.45	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	1
198.46.81.6	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/xmlrpc.php	Block	1
46.19.85.8	Israel	147.237.77.216	dover.idf.il	Multiple Malformed URL from 46.19.85.8	Block	1
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.134	Block	1
79.178.129.119	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
171.25.193.77	Sweden	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
66.249.69.30	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1725	Block	1
50.62.161.179	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
2.54.7.201	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.67.109.195	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.220	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
194.150.113.81	Denmark	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
84.109.105.93	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.93.29	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
46.19.85.8	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
149.202.98.161	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
50.62.176.169	United States	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on maarachot.idf.il/xmlrpc.php	Block	1
50.62.161.45	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
198.46.81.6	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
46.19.85.8	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.8	Block	1
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58623	Block	1
79.180.120.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.210.188.41	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
173.252.90.105	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.69.38	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.69.38	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
2.54.8.227	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1