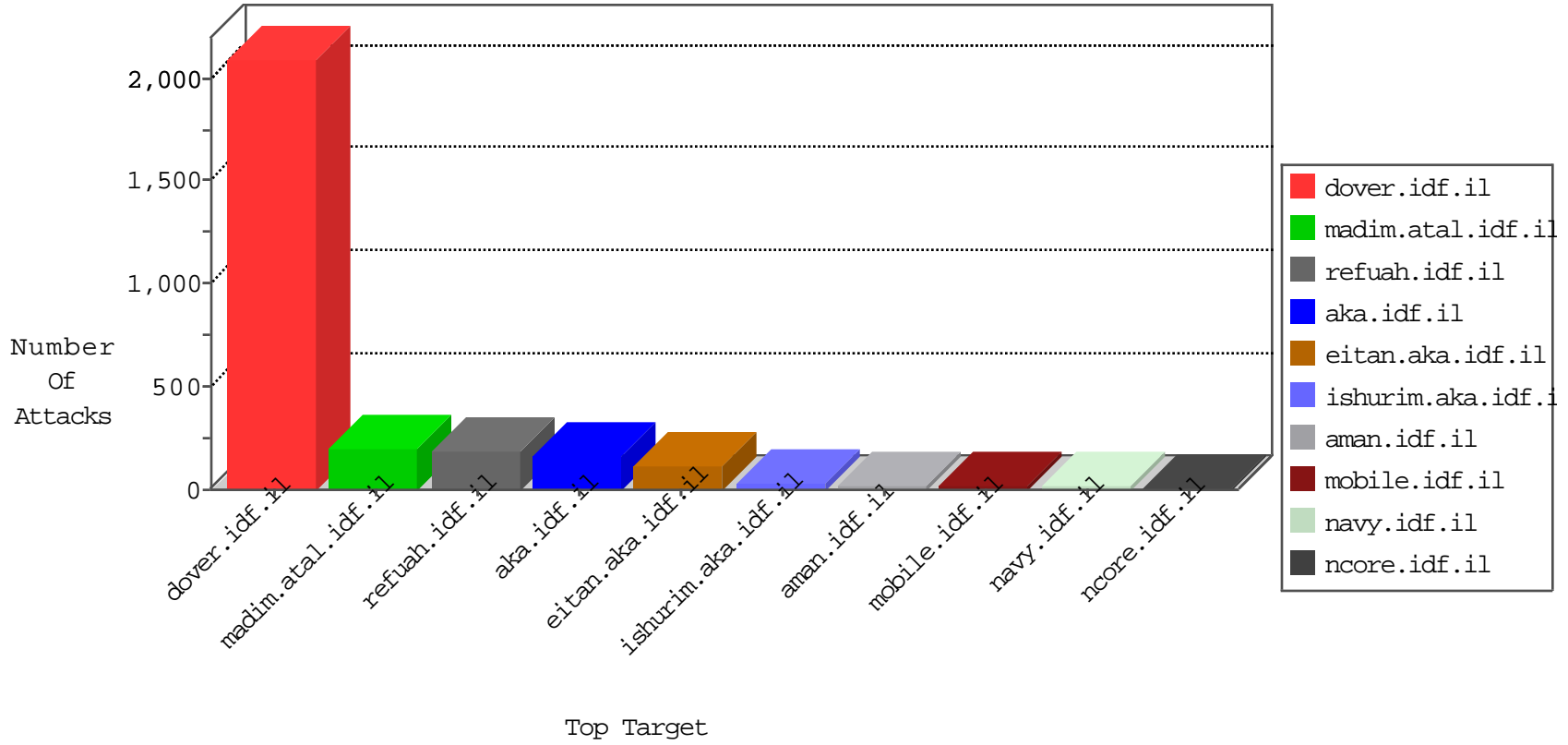


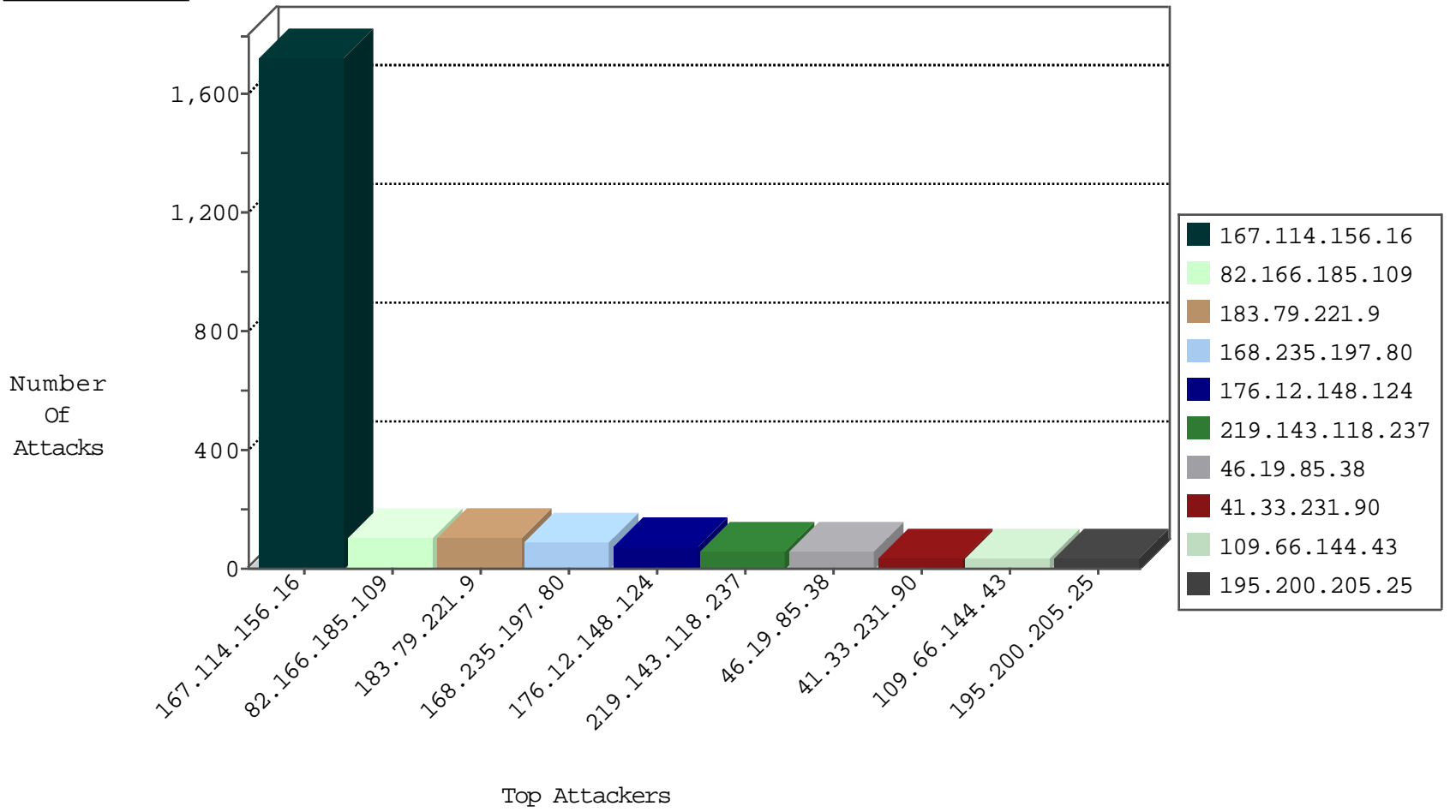
IDF Under Attack Daily Report



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	3158
168.235.197.80	United States	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	28
213.8.129.147	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	14
87.69.52.148	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
109.67.203.38	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
217.132.48.176	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
81.218.105.235	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
115.239.228.8	China	147.237.76.200	eitan.aka.idf.il	JLM_Under_Attack_Con_Http	drop	2
173.195.0.21	United States	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
85.25.43.94	Germany	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
212.179.177.148	Israel	147.237.72.166	aka.idf.il	block-sp-traf1	drop	1
168.235.197.80	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Htps	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

12-14-2015-08:04:00 to 12-14-2015-09:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

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
212.179.177.148	147.237.77.216	Israel	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
174.1.80.244	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.137.26	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.55.233	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.85.31.170	147.237.0.16	Russian Federation	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
166.63.125.149	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
78.193.2.8	147.237.72.167	France	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.146.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
168.235.197.80	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	79
82.166.185.109	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	68
219.143.118.237	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
82.166.185.109	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	33
195.200.205.25	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	32
109.66.144.43	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
2.54.160.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
109.66.144.43	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	15
46.19.86.138	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
80.246.137.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	12
188.165.234.129	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
46.19.86.138	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
5.29.113.35	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.10	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	8
62.0.6.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
46.19.85.21	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
219.143.118.237	China	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
80.246.137.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
183.79.221.9	Japan	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.21.194	Israel	147.237.76.177	noore.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
219.143.118.237	China	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
62.0.6.226	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
62.0.6.226	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
219.143.118.237	China	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
219.143.118.237	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.116.63.198	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.131	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
77.87.228.72	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.42	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	4
176.13.20.230	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.142.138.62	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.131	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.42	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
217.132.48.176	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
213.8.129.147	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
194.114.146.227	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.12.148.124	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.146.177	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
80.246.137.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
31.210.186.195	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.54.153.187	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
62.219.163.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.137.26	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.183.180.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.232.27.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
79.176.225.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.27.105.84	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
176.12.148.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	69
46.19.85.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
183.79.221.9	Japan	147.237.76.200	eitan.aka.idf.il	Multiple Abnormally Long Request from 183.79.221.9	Block	46
183.79.221.9	Japan	147.237.76.200	eitan.aka.idf.il	Multiple Illegal HTTP Version from 183.79.221.9	Block	46
2.54.152.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
79.178.210.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	18
2.54.23.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
176.13.23.230	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	9
79.178.210.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
46.19.86.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
147.236.38.135	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 147.236.38.135	Block	3
194.114.146.227	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
107.178.195.167	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
37.26.147.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.4.240	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.19.57	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.34	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.179.177.148	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 212.179.177.148 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
109.226.48.112	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
84.110.83.177	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	1
37.26.146.156	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
195.200.205.25	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
183.79.221.9	Japan	147.237.76.200	eitan.aka.idf.il	Abnormally Long Request request version	Block	1
176.12.144.243	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
62.90.35.105	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	1
207.241.226.42	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/templates/general/general.aspx	Block	1
40.77.167.98	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
184.105.247.196	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
82.166.185.109	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	1
176.13.21.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.179.177.148	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
95.108.132.166	Russian Federation	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/templates/login/login.aspx	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
80.246.130.154	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz/resources/images/innerpage/goback.gif	Block	1
183.79.221.9	Japan	147.237.76.200	eitan.aka.idf.il	Illegal HTTP Version x`xY x"x"x*x" HTTP/1.0	Block	1
66.249.64.75	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in www.eitan.aka.idf.il/983-en/eitan.aspx	None	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
107.178.195.171	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
2.54.157.247	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.3.146.186	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.94.38.200	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.aspx/getauthuser	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakchal.idf.il/1109-he/nakchal.aspx	Block	1
46.19.86.213	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
147.236.38.135	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1
104.236.113.214		147.237.76.30	himush.idf.il	Unauthorized Method HEAD for /	Block	1
37.26.147.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	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
2.54.16.12	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.130.154	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 80.246.130.154	Block	1