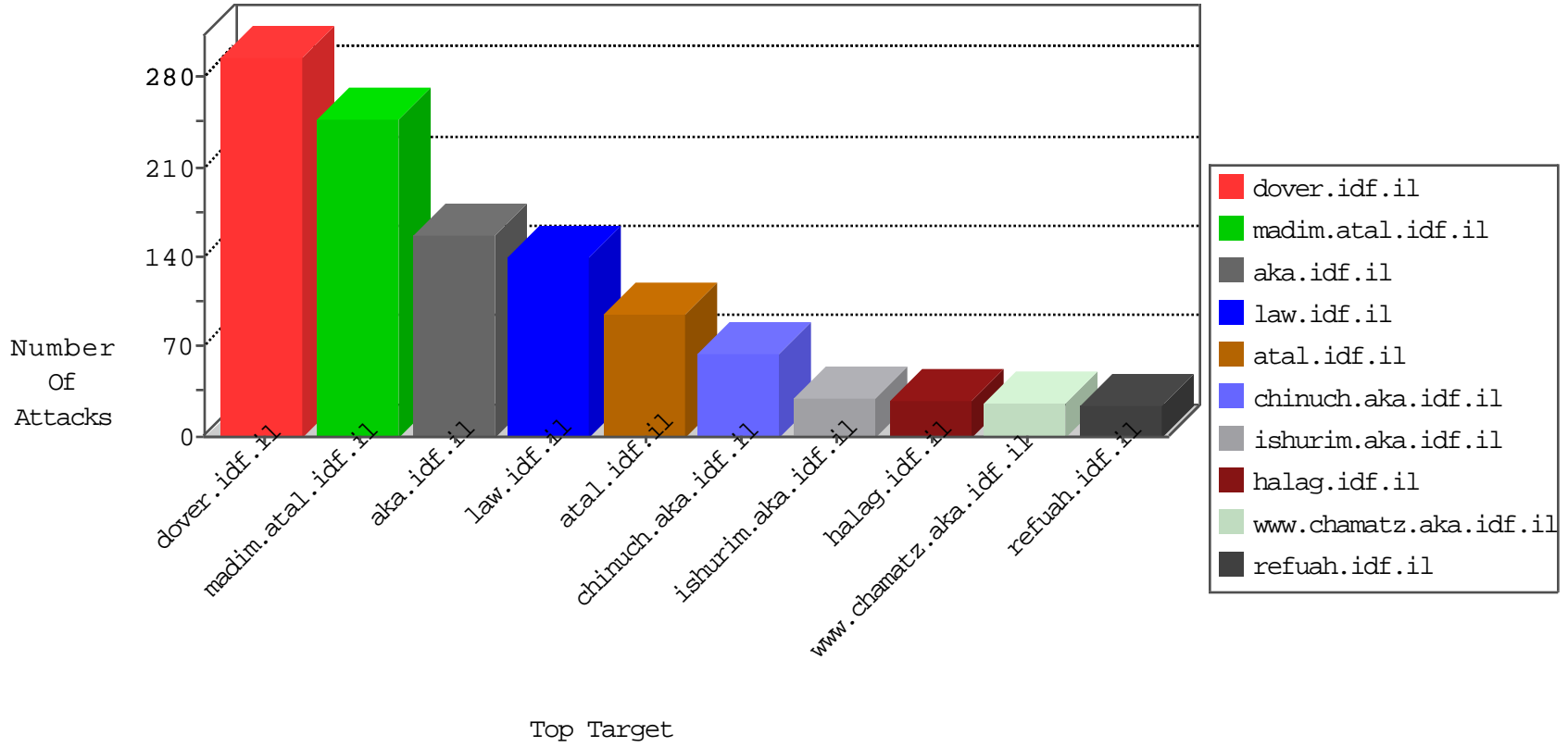


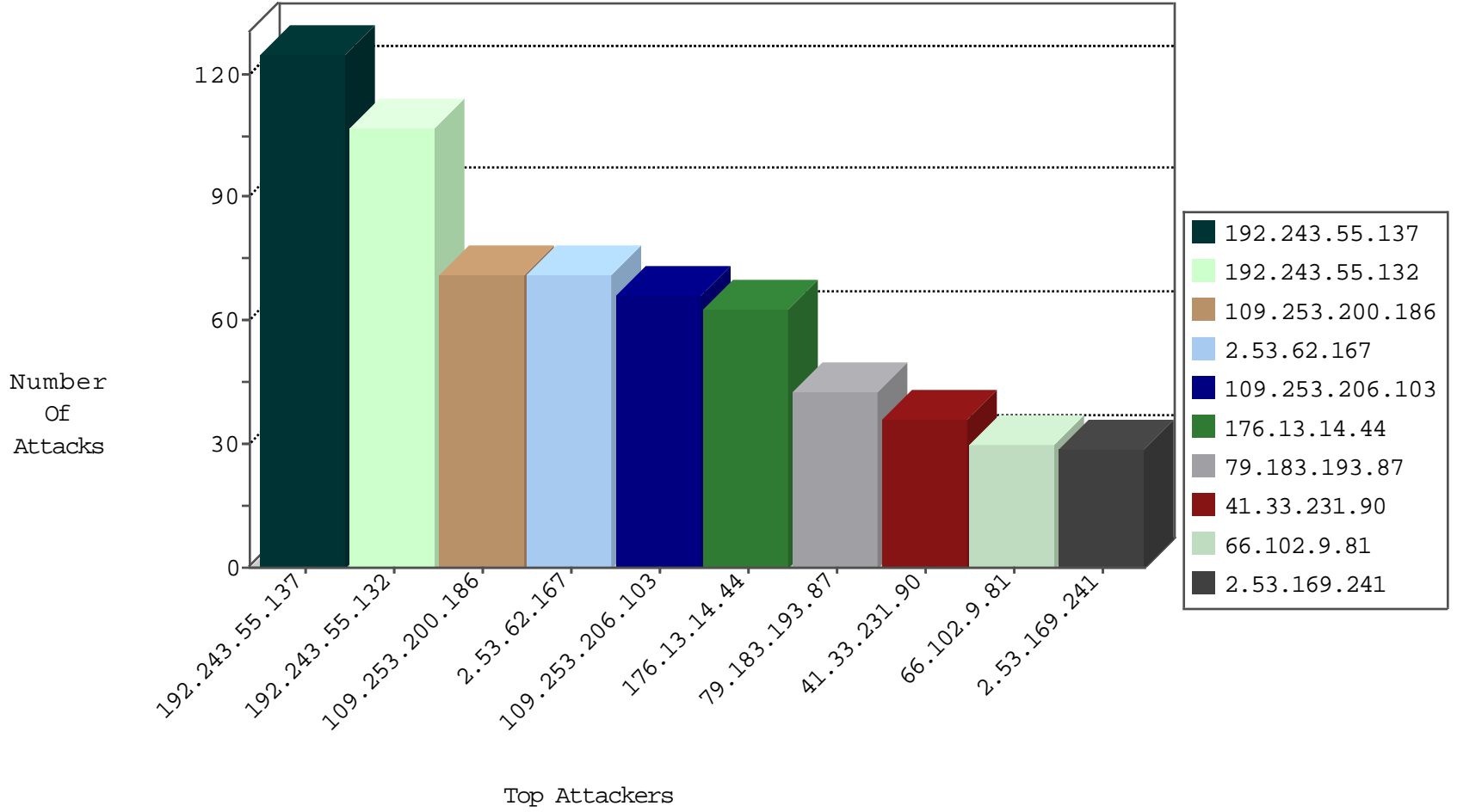
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.243.55.132	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	405
192.114.3.241	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	79
212.29.237.71	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
176.13.22.179	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
79.180.197.110	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
212.150.245.250	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
213.57.126.231	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
46.19.85.32	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.199.226.249	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
162.210.196.97	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
108.59.8.80	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
192.116.48.47	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
157.55.39.215	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
192.118.12.102	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
157.55.39.162	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.102.9.81	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	27
192.116.83.2	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
176.228.5.113	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
139.196.36.18	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
139.196.36.18	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1
109.64.10.221	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.137.251	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.246	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
198.54.90.200	147.237.76.147	United States	chimuch.aka.idf.il	Tehila - Perl LWP with fake user agent	1
192.117.128.217	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
186.119.125.236	147.237.0.16	Colombia	ny-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
176.13.9.51	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
139.196.36.18	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
139.196.36.18	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
79.178.169.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.80.155.215	147.237.77.216	United States	dover.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

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
176.13.14.44	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
79.183.193.87	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	22
79.183.193.87	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
192.243.55.132	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	17
192.243.55.137	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	17
109.64.10.221	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
192.243.55.137	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
192.243.55.132	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
192.243.55.137	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	13
192.243.55.137	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.132	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
192.243.55.132	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
147.236.238.85	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.243.55.132	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
80.178.98.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
147.236.238.85	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
193.169.70.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.243.55.137	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
192.243.55.132	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
94.230.86.143	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
81.218.116.129	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
195.160.242.40	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.89	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
207.46.13.74	United States	147.237.77.233	atal.idf.il	drop	SAM rule	drop	6
37.26.148.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.139.226	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.200.205.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.113.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
147.236.31.63	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.89	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.102.195.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
147.236.31.63	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.89	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.80.196.44	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.89	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.26.148.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.16	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.132	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.117.143.194	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.61	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
66.102.9.101	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.200.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
2.53.62.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	71
109.253.206.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
2.53.169.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	13
2.53.58.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
46.19.85.252	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
81.218.22.216	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
199.30.24.71	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
199.30.24.171	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
85.250.182.89	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mivtza	Block	2
2.55.1.43	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
207.46.13.72	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
219.74.180.185	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.65.237	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1361-10635-he/dover.aspx	Block	1
157.55.39.42	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.42	Block	1
2.55.31.241	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
220.181.108.187	China	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
78.39.133.5	Iran, Islamic Republic of	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
184.105.139.68	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
203.127.58.236	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.75.43	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
157.55.39.42	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
23.81.90.154	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
87.69.160.97	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
79.183.70.226	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
46.19.86.134	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
193.169.70.108	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	1
82.80.198.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
203.127.96.236	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.78.234	Block	1
157.55.39.215	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/general/	Block	1
40.77.167.37	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
1.80.191.113	China	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.69.227.111	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
79.183.193.87	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
49.80.175.175	China	147.237.76.42	refuah.idf.il	Unauthorized Method HEAD for 147.237.76.42/894-he/refuah.aspx	Block	1
193.169.70.108	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/sip_storage/files/8/	Block	1
132.71.100.72	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
84.94.114.184	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
74.91.23.166	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
45.32.233.86	Netherlands	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
157.55.39.217	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.53.16.99	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
87.71.6.0	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/resource/userfollowresource/create/	Block	1
66.249.64.238	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/links/links.aspx	Block	1
149.78.48.105	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.55.31.241	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/general.aspx	Block	1
84.94.211.85	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
77.75.79.54	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/34/	Block	1