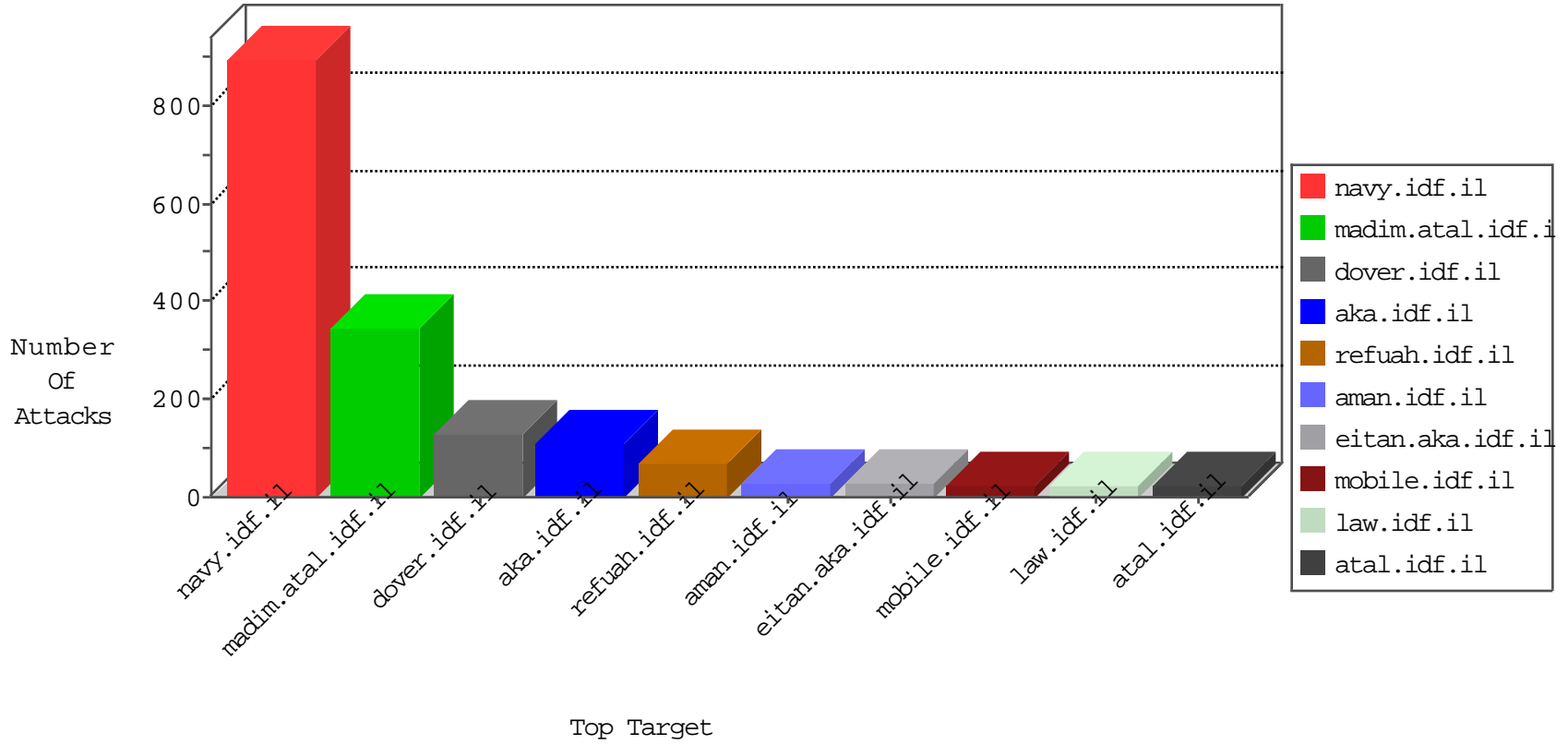


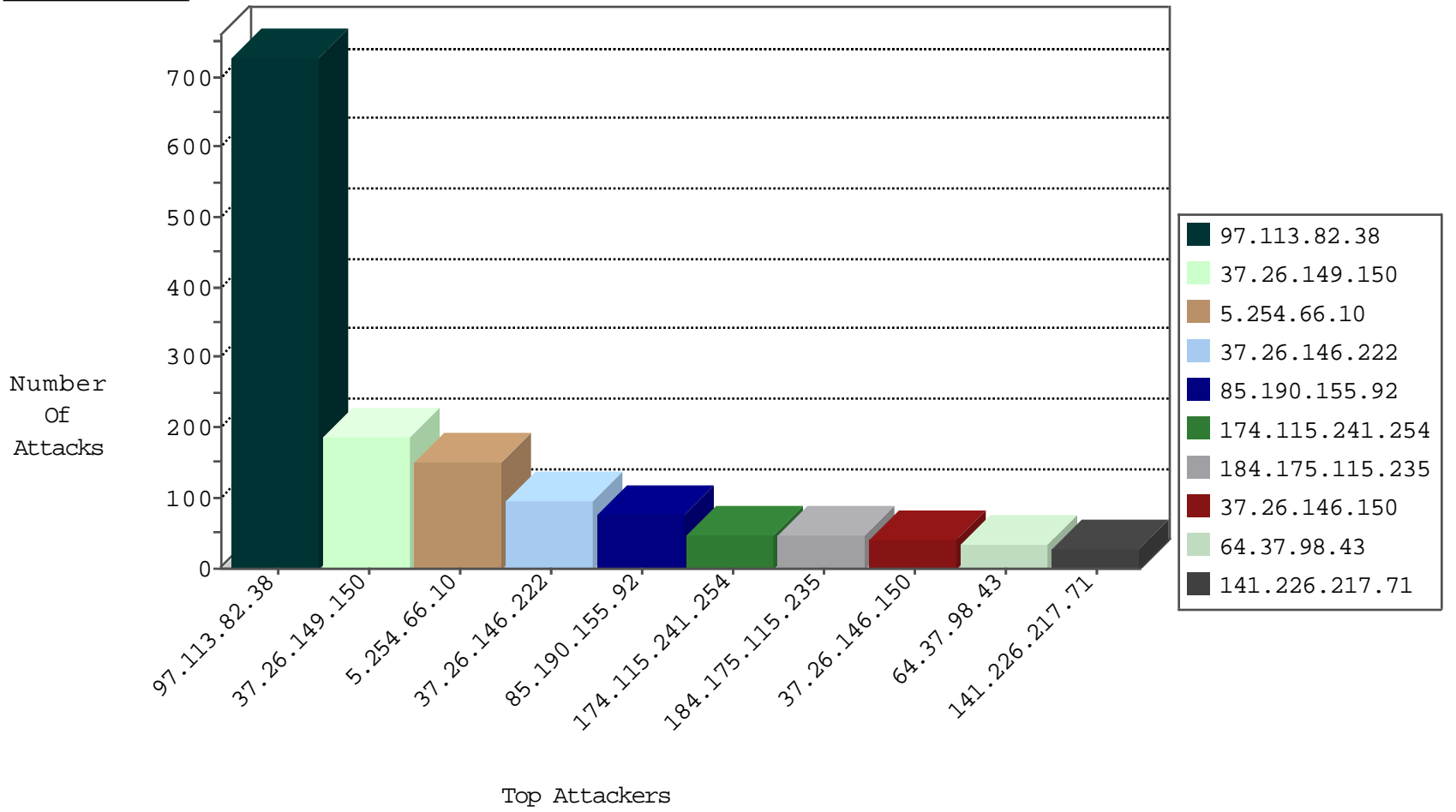
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
115.230.125.146	China	147.237.76.197	e.himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
51.254.172.96	France	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1

09-07-2016-23:04:04 to 09-08-2016-00:04:04

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
91.121.135.78	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
91.121.136.34	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
91.201.236.50	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.50	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
211.141.78.56	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
211.141.78.56	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
85.64.188.142	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
211.141.78.56	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
45.79.103.178	147.237.72.166	United States	aka.idf.il	WEB-MISC Chunked-Encoding transfer attempt	1
193.201.225.149	147.237.8.27	Ukraine	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.94.142	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
93.174.93.46	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.8.14	Ukraine	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
211.141.78.56	147.237.77.234	China	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
85.65.201.101	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
211.141.78.56	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
50.116.123.135	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
195.88.208.193	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.72.217	Netherlands	e.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.94.142	147.237.0.16	Netherlands	my-kosher-kravi.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
97.113.82.38	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	726
141.226.217.71	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
85.190.155.92	Germany	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	24
85.190.155.92	Germany	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	22
85.190.155.92	Germany	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
82.145.221.35	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
86.157.25.94	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	16
5.254.66.10	Romania	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
5.254.66.10	Romania	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
5.254.66.10	Romania	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
5.254.66.10	Romania	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
5.254.66.10	Romania	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
5.254.66.10	Romania	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
5.254.66.10	Romania	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
174.115.241.254	Canada	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
174.115.241.254	Canada	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	13
5.254.66.10	Romania	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
174.115.241.254	Canada	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	13
46.19.85.51	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.177	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
24.129.38.47	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
85.190.155.92	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
46.19.86.52	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
64.37.98.43	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
195.60.235.57	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
37.26.146.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	6
174.115.241.254	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.2	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.185	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.228.49.82	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
2.53.14.186	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.86.185	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.146.197	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		alert	6
46.19.85.177	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.103	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
176.13.1.249	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
212.150.174.180	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
85.64.215.125	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
138.246.253.19	Germany	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
37.26.149.150	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		monitor	4
46.19.85.126	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
217.132.114.119	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
5.254.66.10	Romania	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.86.227	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.254.66.10	Romania	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
109.253.200.63	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.32.179.236	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
184.175.115.235	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
5.254.66.10	Romania	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
5.254.66.10	Romania	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	178
37.26.146.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	96
37.26.146.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
152.23.35.170	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/smalim/smalim.aspx	Block	3
213.151.63.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.55.38.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.61	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
89.138.200.207	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
46.42.130.135	Russian Federation	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
37.26.146.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
85.65.135.0	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatgauntity.aspx	Block	2
66.102.9.5	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/klali.aspx	Block	2
37.26.146.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.139.173.120	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	2
66.249.69.83	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/9/70679.pdf	Block	1
180.97.106.37	China	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 180.97.106.37 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
141.226.217.71	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
79.177.2.183	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
213.57.229.160	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$questionUpdate\$txtOtherQuestion in www.aka.idf.il/main/gyius/faq.aspx	None	1
176.228.49.82	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1275-he/atal.aspx	Block	1
66.249.69.119	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/gyius/forum/asp/showforum.asp	Block	1
180.97.106.37	China	147.237.77.226	www.chamatz.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
79.180.132.223	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
2.53.167.37	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
180.97.106.37	China	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
89.139.185.139	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
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/brothers/skira/default.asp	Block	1
180.97.106.161	China	147.237.0.16	my-kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
157.55.39.49	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.49	Block	1
66.102.9.3	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
180.97.106.37	China	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
89.237.99.66	France	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/5/63635.pdf	Block	1
185.3.147.86	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	1
37.26.147.186	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
157.55.39.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
85.65.229.130	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
180.97.106.37	China	147.237.0.34	tikshuv.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
109.65.186.42	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1
204.79.180.181	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/default.aspx	Block	1
157.55.39.115	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
87.68.13.247	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1