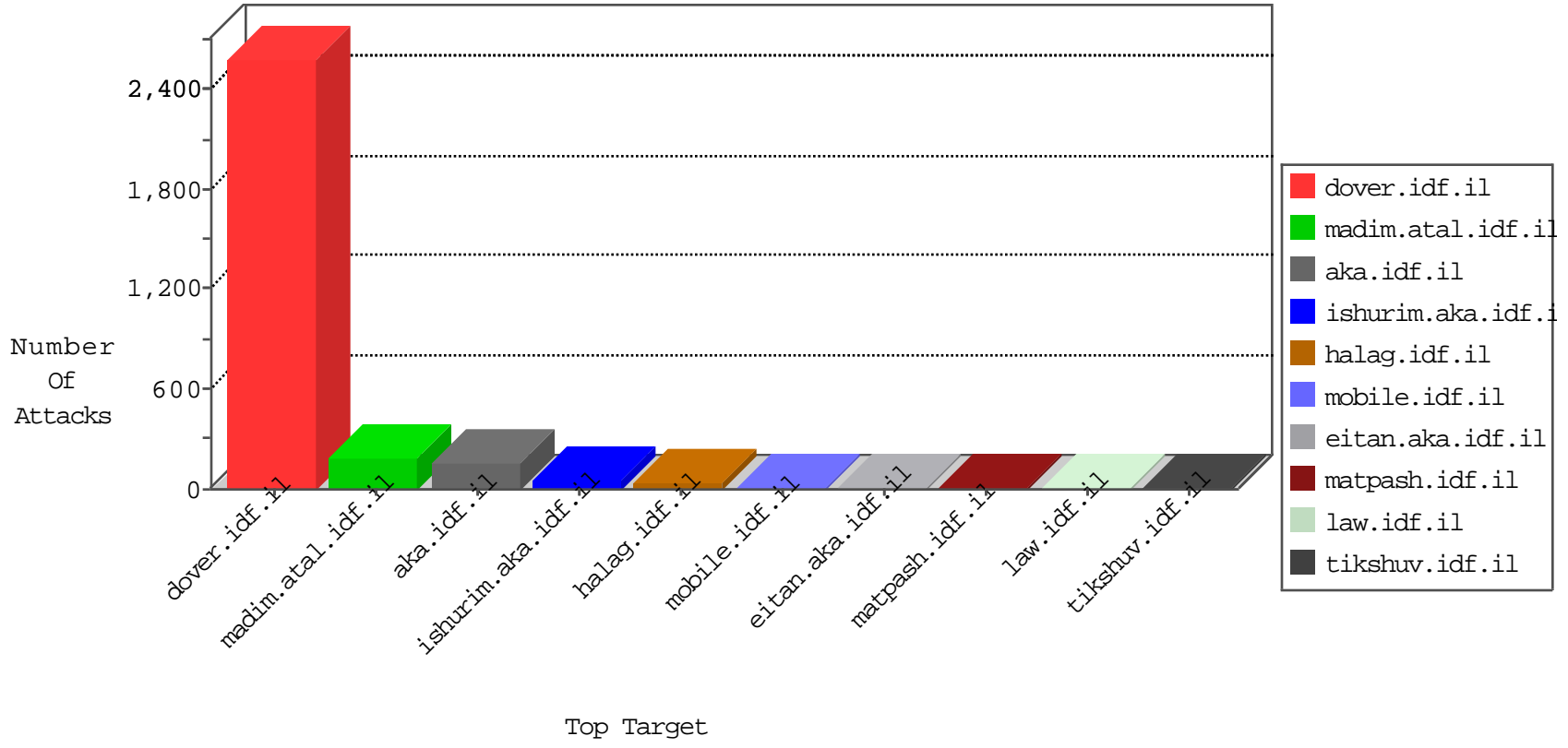


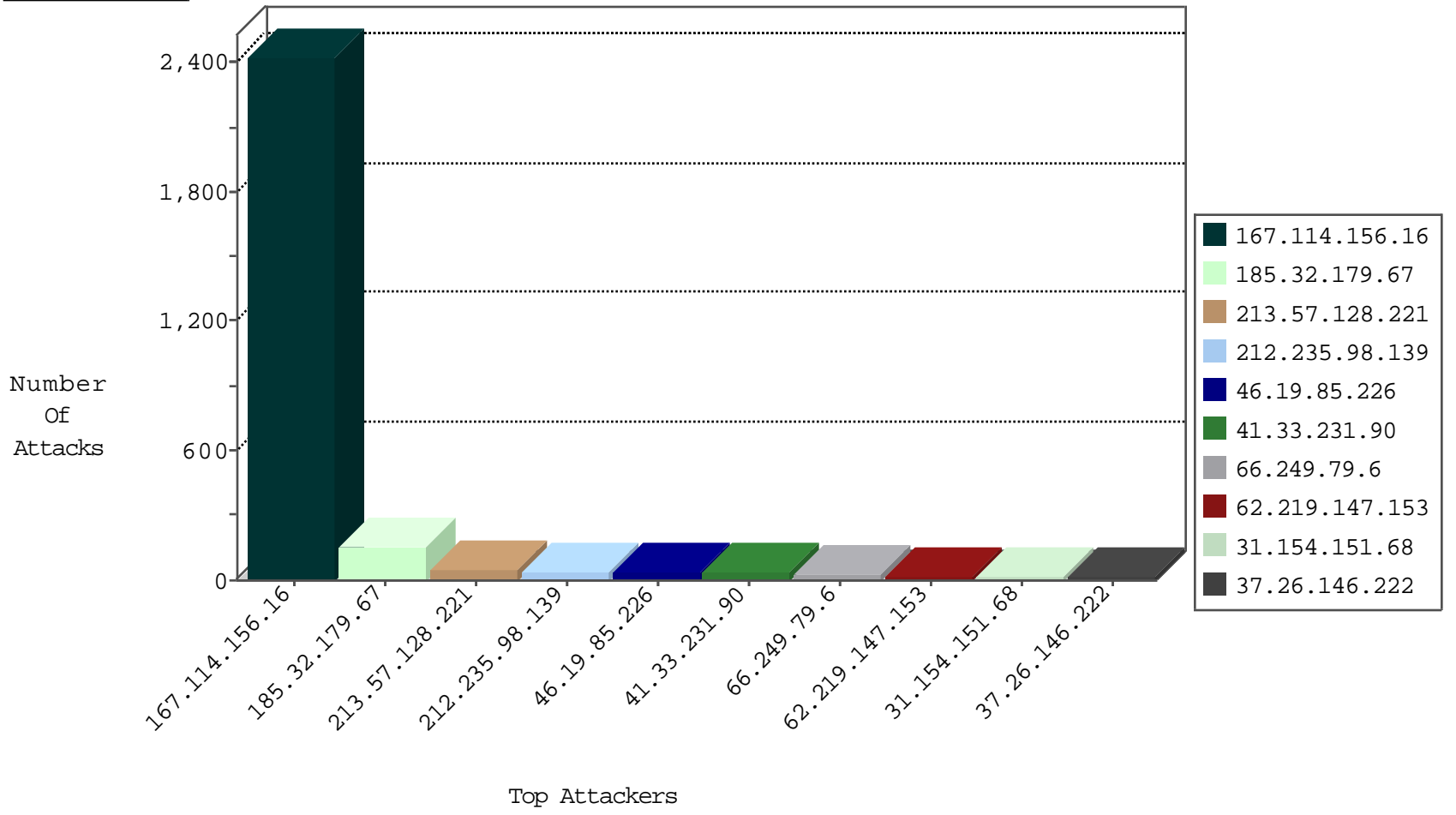
IDF Under Attack Daily Report



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	3417
66.249.79.127	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2675
109.67.107.19	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
84.229.132.170	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
93.173.136.254	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
94.102.49.210	Netherlands	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
80.82.78.207	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
158.69.199.64	United States	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.210	Netherlands	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
107.150.55.51	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	drop	1
94.102.49.210	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
180.97.106.36	China	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.210	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
80.82.78.207	Netherlands	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
109.248.80.15	Russian Federation	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.210	Netherlands	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1

12-11-2015-08:04:02 to 12-11-2015-09:04:02

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
82.205.115.81	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	2
185.32.179.67	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	1
118.26.233.57	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
118.26.233.57	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
118.26.233.57	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
64.38.133.137	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
118.26.233.57	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
118.26.233.57	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
118.26.233.57	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
114.34.237.10	147.237.8.14	Taiwan	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
82.127.85.8	147.237.77.216	France	dover.idf.il	ET SCAN NMAP -sS window 1024	1
212.179.177.148	147.237.72.167	Israel	ishurim.aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.235.98.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	40
46.19.85.226	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
66.249.79.6	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
213.57.128.221	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	29
213.57.128.221	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	22
62.219.147.153	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
37.26.146.222	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
89.138.245.84	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.154.151.68	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
84.228.242.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.154.151.68	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
149.88.34.208	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.142.200.240	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.54.155.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.50.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.46.13.57	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.23	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.142.200.240	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
2.52.136.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.44.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.254.1	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.22.205	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.143.142.57	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.183.112.216	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
5.29.157.161	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
157.55.39.173	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
80.187.102.152	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.54.181.19	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
37.142.68.40	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
207.46.13.151	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
128.232.110.28	United Kingdom	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
85.250.230.150	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
46.19.85.103	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
62.210.215.120	France	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
66.249.64.243	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
157.55.39.61	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
195.154.227.118	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
46.19.86.124	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
84.229.132.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.243	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.142.68.13	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
180.97.106.161	China	147.237.77.205	prisha.idf.il	drop	SAM rule	drop	1
213.57.224.248	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.105	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
38.99.82.216	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
180.97.106.162	China	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	1
74.82.47.11	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.32.179.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
185.32.179.67	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 185.32.179.67	Block	54
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/\$\$\$&?&?\$\$\$	Block	9
176.12.142.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
46.19.85.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
37.26.149.245	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.125.141.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.5.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.68.254.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/asp/giyus.asp	Block	2
117.202.4.222	India	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
117.202.4.222	India	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	2
79.183.112.216	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
77.40.129.123	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
184.105.247.195	United States	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on 147.237.0.19/	Block	1
85.164.131.194	Norway	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.183.3.155	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.133	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/modules/forums.frm/frmsendmessage.aspx	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
83.71.247.37	Ireland	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.64.234	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-9067-he/atal.aspx	Block	1
85.164.131.194	Norway	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
40.77.167.16	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atall/izkor/view_imgtop.asp	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.140	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/modules/forums.frm/frmpintmessage.aspx	Block	1
46.19.86.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
84.94.171.6	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.28.121	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.178.140.154	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding md in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
164.138.115.134	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/894-he/nakhal.aspx	Block	1
66.249.65.112	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/3272.jpg	Block	1
40.77.167.57	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
212.179.177.148	Israel	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
80.86.94.7	Germany	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/sitemap/sitemap.aspx	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1153-20505-he/kkkkkkk=e33525cdkkkkkkkk_e33525cd	Block	1
46.166.139.20	Netherlands	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
85.164.131.194	Norway	147.237.77.74	law.idf.il	PHP Attempt	Block	1
2.54.188.141	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.178.140.154	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 79.178.140.154	None	1
195.5.25.146	Ukraine	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
165.138.36.2	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/5/2685.jpg	Block	1
95.45.254.122	Ireland	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
46.19.85.165	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
213.57.216.109	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1