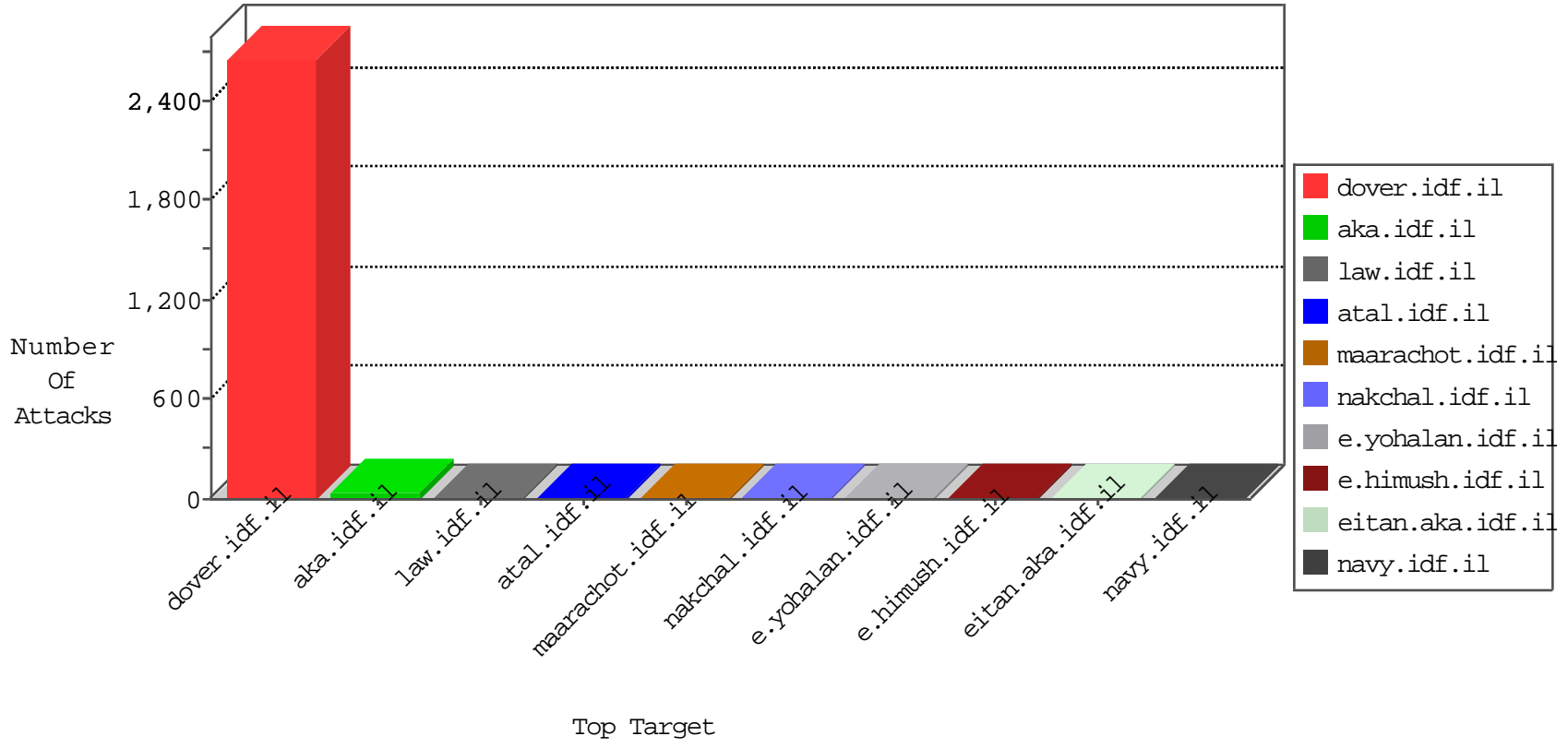


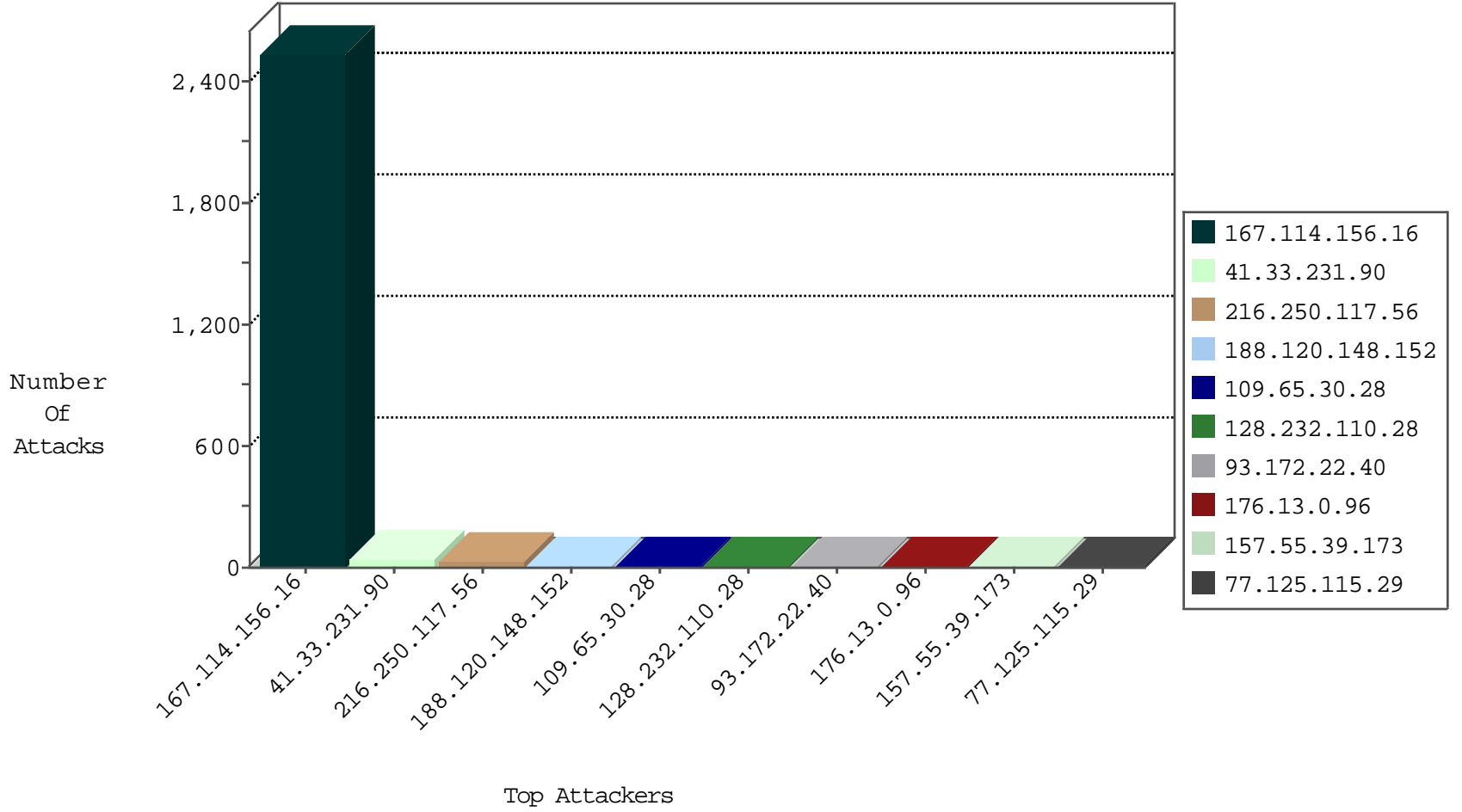
# IDF Under Attack Daily Report



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	3311
222.186.56.115	China	147.237.0.35	akaws.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
204.42.253.132	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1

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

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
216.250.117.56	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
216.250.117.56	147.237.77.216	United States	dover.idf.il	LOCAL_RULES access attempt to file_manager.php	2
66.249.66.81	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
162.253.66.6	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
88.249.106.23	147.237.76.177	Turkey	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
45.55.198.52	147.237.0.16		my-kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
222.186.56.115	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
187.161.112.233	147.237.76.198	Mexico	e.yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
186.88.19.160	147.237.76.199	Venezuela	e.nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
113.58.100.255	147.237.76.30	China	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.102.48.195	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
222.186.56.115	147.237.76.86	China	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
187.160.181.25	147.237.0.16	Mexico	my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
109.65.30.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.120.148.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
93.172.22.40	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
77.125.115.29	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	4
37.140.141.35	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.243.19	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.173	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.26.146.195	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
128.232.110.28	United Kingdom	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
46.19.86.42	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
128.232.110.28	United Kingdom	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
66.249.66.90	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
128.232.110.28	United Kingdom	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
80.246.133.48	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
188.120.148.181	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.117.128.81	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.126	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.94	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.31	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.124	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.33	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.210	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
2.54.184.136	Israel	147.237.76.42	refuah.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	1
141.212.122.112	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
80.246.133.48	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
212.14.228.214	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.117.128.81	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.126	United States	147.237.77.61	e.cogat.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.102	United States	147.237.0.33	idf.il	drop		drop	1
74.82.47.31	United States	147.237.76.148	ggcenter.aka.idf.il	drop		drop	1
184.105.247.208	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.210	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.29.164.247	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.115	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.120.57.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.91	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.142.160.95	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.127	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.51	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
188.120.148.152	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.19.86.42	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.211	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.29.164.247	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.116	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
213.8.204.14	Israel	147.237.72.167	ishurim.aka.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
216.250.117.56	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
216.250.117.56	United States	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 216.250.117.56	Block	5
216.250.117.56	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 216.250.117.56	Block	5
176.13.0.96	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	4
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	2
84.109.130.240	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	2
213.8.204.45	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1362-he/dover.aspx	Block	2
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
79.179.99.94	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
213.57.231.97	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
45.55.198.52		147.237.0.15	kosher-kravi.idf.il	Distributed Unauthorized URL Access on /	Block	1
183.79.220.223	Japan	147.237.77.74	law.idf.il	Parameter Type Violation SearchText in www.law.idf.il/163-6639-he/patzar.aspx	Block	1
149.255.228.66	Iraq	147.237.77.74	law.idf.il	PHP Attempt	Block	1
104.131.168.154	United States	147.237.76.30	himush.idf.il	Unauthorized Method HEAD for /	Block	1
216.250.117.56	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/admin/categories.php/login.php	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
2.52.31.28	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	1
157.55.39.222	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/109335.pdf x³xÿÄ¿Ä½x³Ä?~x³xÿ Ä¿Ä½x³xÿÄ¿Ä½x³Ä x³xÿÄ¿Ä½x³xÿÄ¿Ä½	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.179.99.94	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
216.250.117.56	United States	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
45.55.198.52		147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on /	Block	1
183.79.220.223	Japan	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/228-he/faq.aspx	Block	1
149.255.228.66	Iraq	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
104.131.168.154	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to /	Block	1
208.115.111.73	United States	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
66.249.66.126	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/71857-he/maarachot.aspx	Block	1
2.52.63.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.253	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 157.55.39.253	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
188.120.148.152	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
66.249.66.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.78	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
104.131.168.154	United States	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on /	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.79	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/1074-he/x?x'xf "x~x" x xœx·x'x"m"x " x·x"xœx·x'x"m"x; x~x"m"x§x".aspx	Block	1
2.54.52.102	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.253	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/plugins/system/ice_speed/	Block	1
141.212.122.112	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to /x	Block	1
89.216.77.209		147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
195.154.146.225	France	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	1
66.249.66.31	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	Block	1
157.55.39.173	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	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
37.26.147.153	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
141.212.122.112	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to /x	Block	1
89.216.77.209		147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	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
66.249.66.43	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1153-14220-he/dover.aspx	Block	1