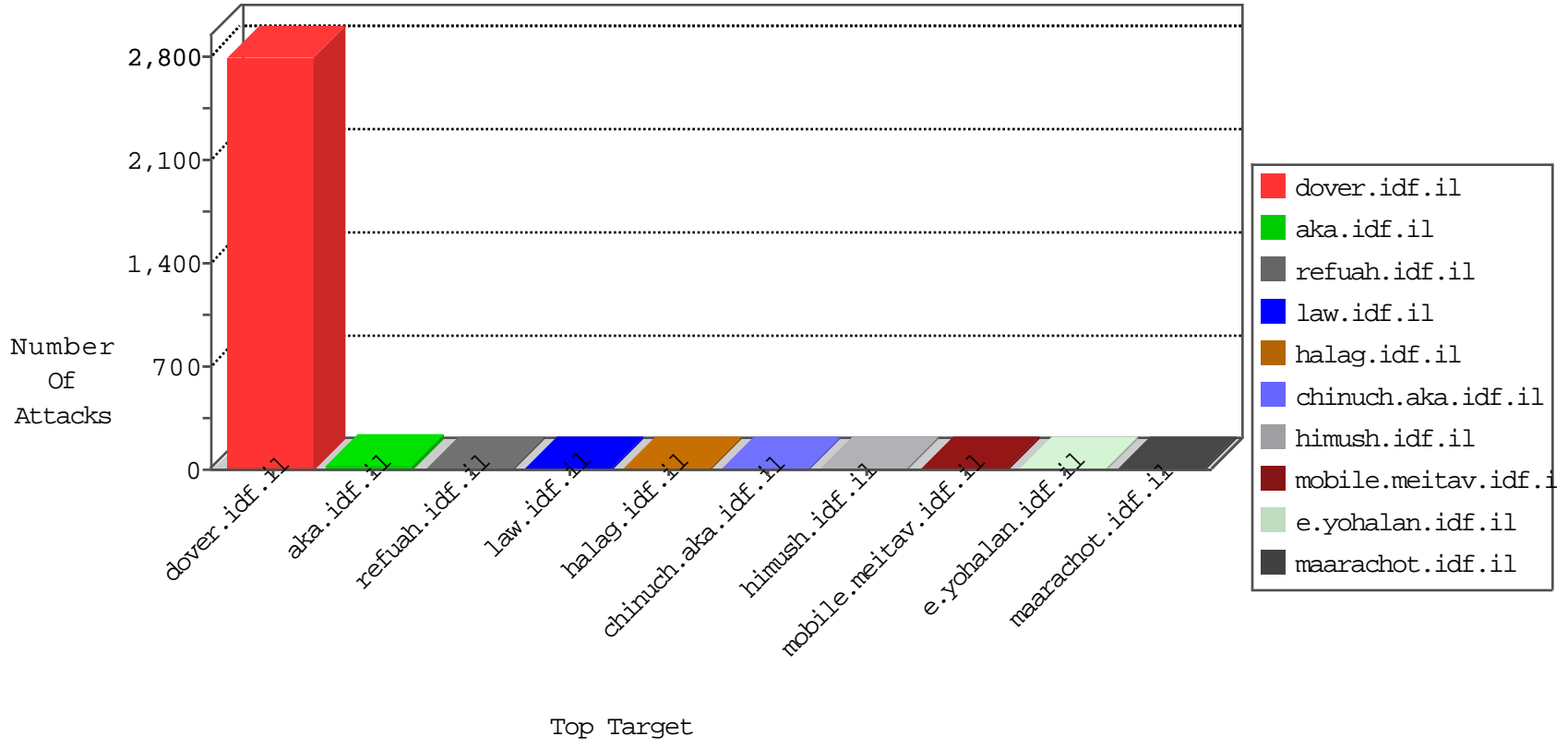


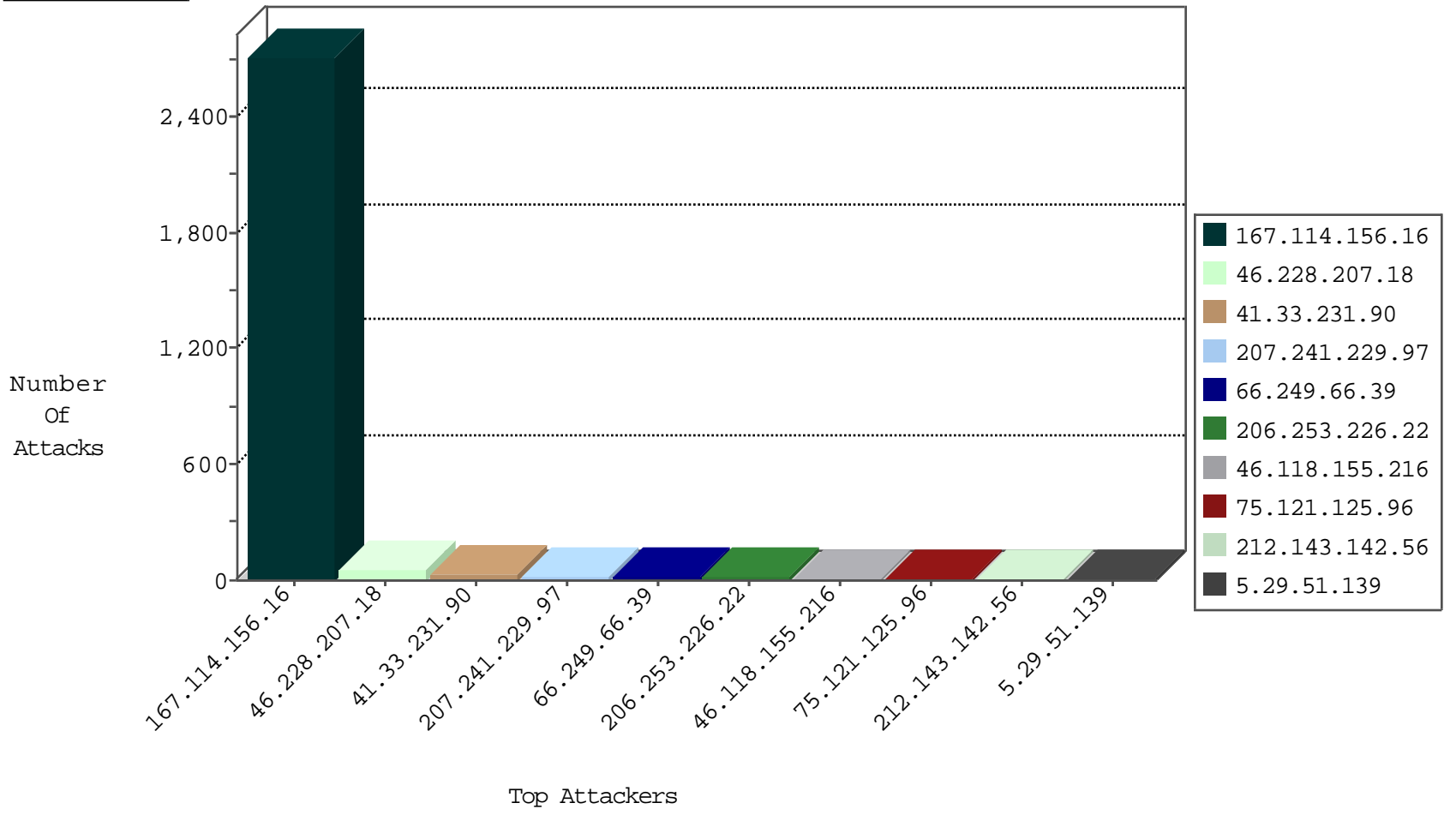
IDF Under Attack Daily Report



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	3434
66.249.64.165	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	202
202.112.51.96	China	147.237.76.30	himush.idf.il	block-sp-traf1	drop	1
84.244.21.221	Russian Federation	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1

12-05-2015-05:04:01 to 12-05-2015-06:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.215.122	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.228.207.18	147.237.76.148	Germany	ggcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
46.228.207.18	147.237.76.198	Germany	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
46.228.207.18	147.237.76.44	Germany	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
46.228.207.18	147.237.76.39	Germany	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
46.228.207.18	147.237.76.200	Germany	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	4
46.228.207.18	147.237.76.38	Germany	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
46.228.207.18	147.237.76.34	Germany	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
46.228.207.18	147.237.76.30	Germany	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
46.228.207.18	147.237.76.196	Germany	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
46.228.207.18	147.237.76.176	Germany	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
46.228.207.18	147.237.76.147	Germany	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	3
46.228.207.18	147.237.76.42	Germany	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
66.249.66.75	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
46.228.207.18	147.237.77.19	Germany	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
46.228.207.18	147.237.76.31	Germany	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.228.207.18	147.237.76.201	Germany	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.228.207.18	147.237.0.35	Germany	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.228.207.18	147.237.76.199	Germany	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.228.207.18	147.237.0.19	Germany	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.228.207.18	147.237.76.197	Germany	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.63.153.251	147.237.8.28	Russian Federation	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.228.207.18	147.237.76.177	Germany	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
81.169.251.74	147.237.8.24	Germany	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
46.228.207.18	147.237.77.235	Germany	sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.228.207.18	147.237.76.202	Germany	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.228.207.18	147.237.0.33	Germany	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.228.207.18	147.237.0.16	Germany	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
208.69.31.46	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.77.205	Netherlands	prisha.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
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
207.241.229.97	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	13
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
75.121.125.96	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
206.253.226.22	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
37.18.51.250	Russian Federation	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
5.29.51.139	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
206.253.226.22	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
77.237.138.51	Czech Republic	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
5.29.51.139	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
206.253.226.22	United States	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
37.46.39.11	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
195.154.227.118	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
206.253.226.22	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
206.253.226.22	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
207.241.229.97	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
184.105.247.248	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
138.32.168.53	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
50.87.144.145	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.86	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.75	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
195.62.53.168	Russian Federation	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
138.32.168.53	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.92	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.54.83.214	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.154.226.90	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
141.212.121.185	United States	147.237.0.35	akaws.idf.il	drop		drop	1
216.218.206.106	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.186.144.109	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
209.126.116.147	United States	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
141.212.121.186	United States	147.237.0.35	akaws.idf.il	drop		drop	1
74.82.47.27	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.106	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.211	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
124.13.27.18	Malaysia	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
141.212.122.74	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.56	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.118.155.216	Ukraine	147.237.76.147	chinuch.aka.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
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	2
176.13.2.149	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	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	2
124.13.27.18	Malaysia	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.78.242	Block	1
66.249.66.40	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-20315-he/dover.aspx	Block	1
46.118.155.216	Ukraine	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/xmlrpc.php	Block	1
199.16.156.124	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/7/size220x0/17467.jpg	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
66.249.66.72	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/fsfg.aspx	Block	1
66.220.156.122	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
141.212.122.64	United States	147.237.77.235	sviva.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
82.166.228.10	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	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
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	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
113.176.180.115	Vietnam	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
66.249.67.142	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/size100x0/2973.jpg	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
66.249.66.28	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.66.28	Block	1
5.255.253.151	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
90.149.67.73	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/haredim/general.aspx	None	1
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
207.46.13.67	United States	147.237.76.30	himush.idf.il	Multiple Unauthorized URL Access from 207.46.13.67	Block	1
113.176.180.115	Vietnam	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
66.249.67.254	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/1/2271.jpg	Block	1
66.249.66.28	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/idf/console/search_resources.aspx	Block	1
181.223.1.198	Brazil	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	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
66.249.66.64	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/72089-he/maarachot.aspx	Block	1
207.46.13.67	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/imagevideogallerylobby/imagevideogallerylobby.aspx	Block	1
124.13.27.18	Malaysia	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/images/shared/home.png	Block	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18858-he/dover.aspx	Block	1
46.118.155.216	Ukraine	147.237.76.147	chinuch.aka.idf.il	PHP Attempt	Block	1
181.223.1.198	Brazil	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
66.249.66.72	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.66.72	Block	1
207.46.13.97	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.maarachot.idf.il/pdf/files/5/109335.pdfx•Â»Âçx"xÿÄ¿Â½Â»x"xÿÄ¿Â½Â»-x"xÿÄ¿Â½Â»x"xÿÄ¿Â½Â»x•Â»Âçx"xÿÄ¿Â½Â»x"xÿÄ¿Â½Â»	Block	1
46.118.155.216	Ukraine	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/blog/	Block	1