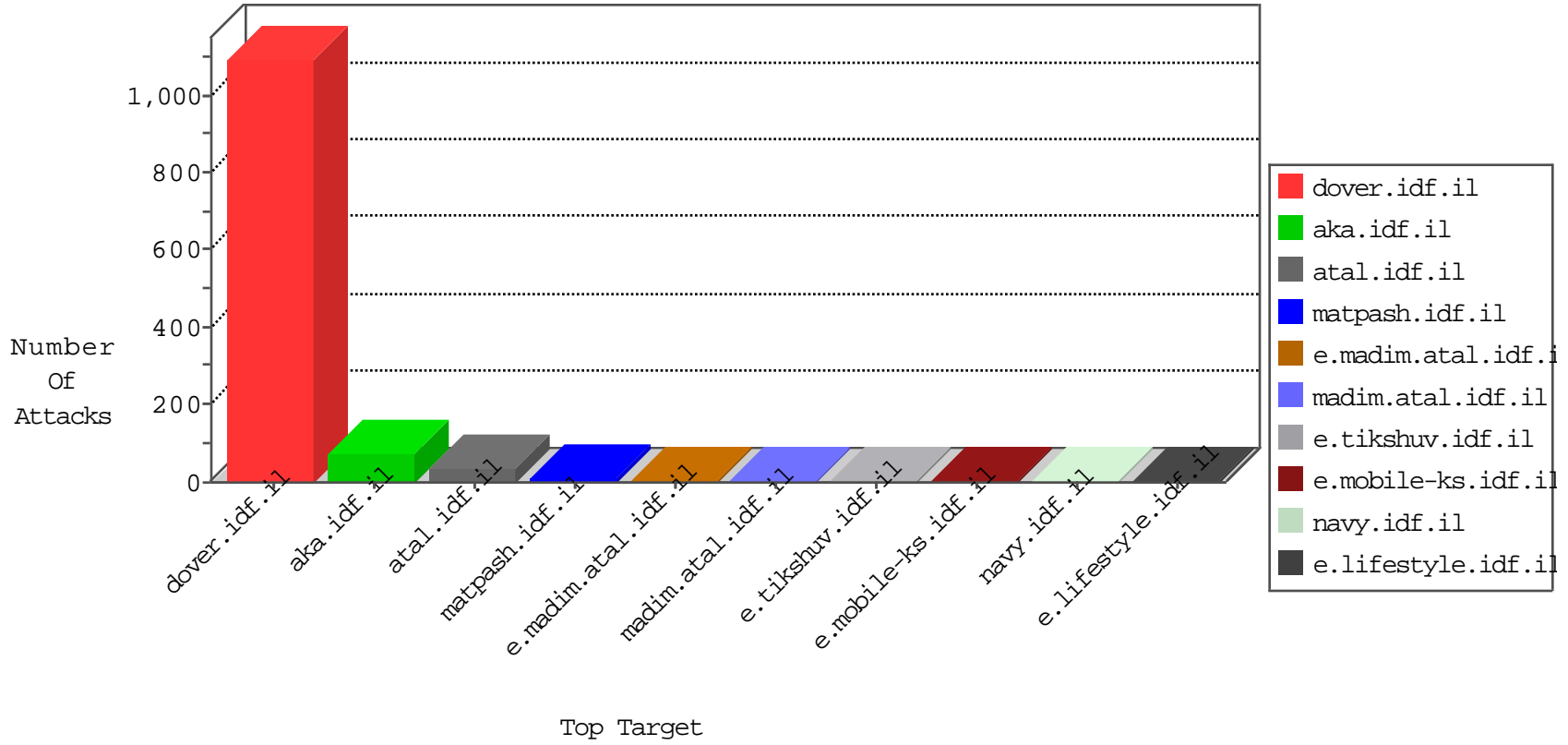


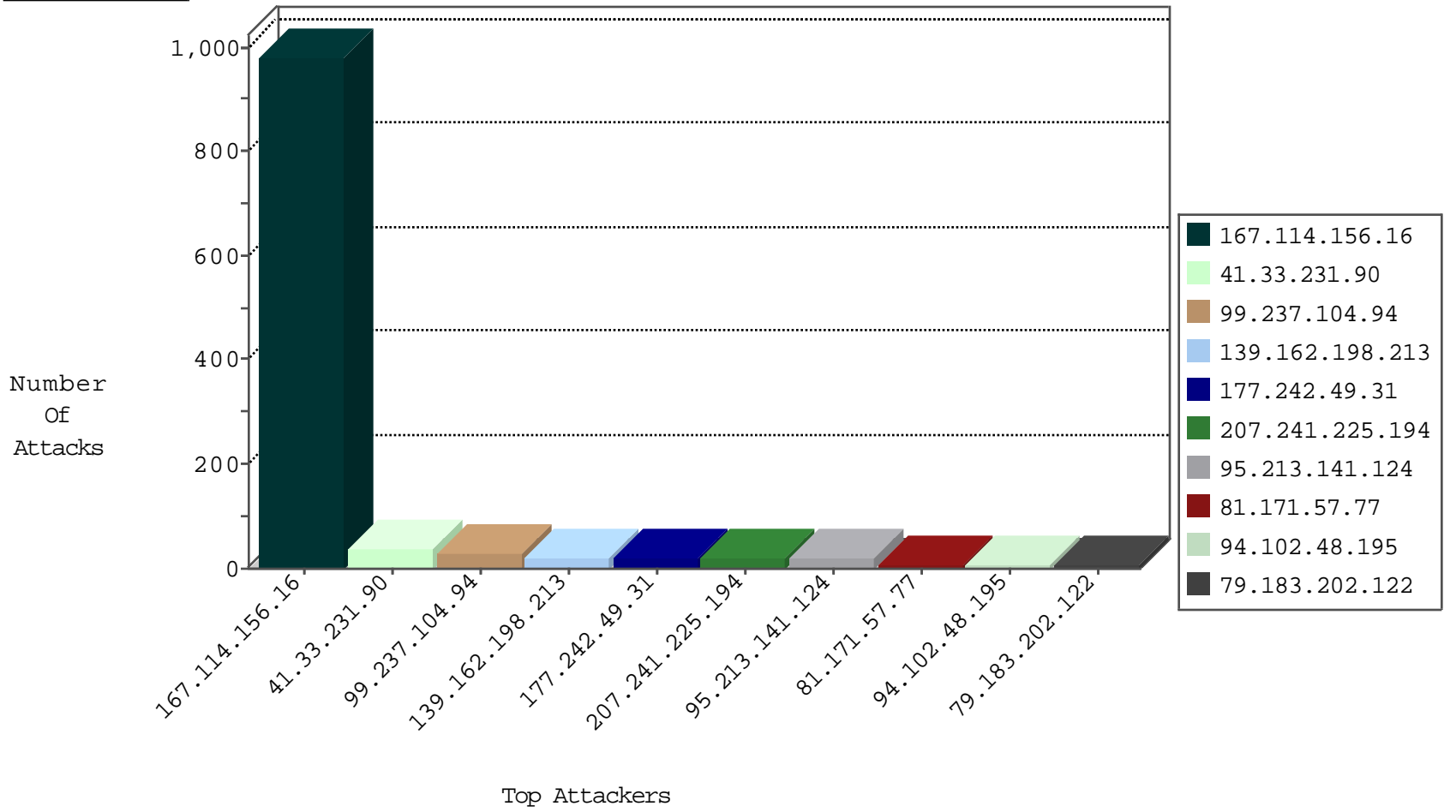
IDF Under Attack Daily Report



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	3525
23.95.248.111	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
89.248.174.4	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1

01-10-2016-05:04:06 to 01-10-2016-06:04:06

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	4
66.249.64.169	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
220.231.195.122	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -f -sS	1
195.154.90.21	147.237.0.34	France	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
159.203.125.110	147.237.0.16	United States	my-kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
104.128.144.131	147.237.72.166	Canada	aka.idf.il	ET SCAN NMAP -sS window 4096	1
83.146.113.205	147.237.76.30	Russian Federation	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
14.54.160.93	147.237.76.30	Korea, Republic of	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
220.231.195.122	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -sS window 2048	1
195.154.90.21	147.237.77.226	France	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
115.182.249.11	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
220.231.195.122	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -sS window 4096	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
99.237.104.94	Canada	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
139.162.198.213	Netherlands	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
95.213.141.124	Russian Federation	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	18
207.241.225.194	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	18
99.237.104.94	Canada	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
81.171.57.77	Netherlands	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
79.183.202.122	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
177.242.49.31	Mexico	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
100.36.168.5	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
177.242.49.31	Mexico	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
177.242.49.31	Mexico	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
177.242.49.31	Mexico	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
177.242.49.31	Mexico	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
79.181.184.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.142.82	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
125.46.26.253	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
173.252.113.115	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
40.127.178.111	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
173.252.113.118	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
108.84.130.87	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.130.5.247		147.237.0.19	madim.atal.idf.il	drop	SAM rule	drop	1
94.102.48.195	Netherlands	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
184.105.139.99	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.20.31	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
94.102.48.195	Netherlands	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.130.5.231		147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
81.169.237.146	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
173.2.20.238	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
185.130.5.247		147.237.0.33	idf.il	drop	SAM rule	drop	1
94.102.48.195	Netherlands	147.237.76.148	ggcenter.aka.idf.il	drop	SAM rule	drop	1
184.105.139.103	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
61.242.114.152	China	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.86	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
94.102.48.195	Netherlands	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
185.130.5.231		147.237.76.202	e.halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.67	United States	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
173.2.20.238	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
104.128.144.131	Canada	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.130.5.247		147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
94.102.48.195	Netherlands	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	1
184.105.247.199	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.29.231.80	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
185.130.5.231		147.237.77.216	dover.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
2.54.174.199	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
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
192.243.55.136	Dominica	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/gyius/kadatz	Block	1
139.162.198.213	Netherlands	147.237.72.166	aka.idf.il	Too Many Cookies in a Request - 138 cookies	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docid in www.aka.idf.il/main/gyius/general.aspx	None	1
37.187.57.8	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
196.40.97.8	South Africa	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
192.243.55.131	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.131	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
207.46.13.45	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/gyius/qanda/default.asp	None	1
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international-training	Block	1
157.55.39.2	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/gyius/general.aspx	None	1
37.187.57.8	France	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
198.57.209.102	United States	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
192.243.55.133	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.133	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
207.46.13.158	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/i/js_inst	Block	1
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	1
195.154.227.118	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
159.203.125.110	United States	147.237.0.16	my-kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
93.172.240.106	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding 3V4J%\$qt(!SY:s38HW>1o3LQQ(L8@eZ/chvanZH.5>oc{O\$R PR in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
37.187.57.8	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
198.57.209.102	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
192.243.55.133	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gyius/kadatz	Block	1
107.178.195.171	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/idf/templates/innerpage.aspx	Block	1
37.26.148.157	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
195.154.227.118	France	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 195.154.227.118	Block	1
176.13.20.31	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
93.172.250.134	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	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
66.249.64.9	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/speakerofmatpash/pages/mangeno nkitzbaotpensya.aspx	Block	1
192.243.55.133	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/gyius/general.aspx?catid=59330&docid=64983	Block	1
107.178.195.171	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.66.125	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
37.187.57.8	France	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
196.40.97.8	South Africa	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
176.13.23.58	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
99.237.104.94	Canada	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.65.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/3288.jpg	Block	1