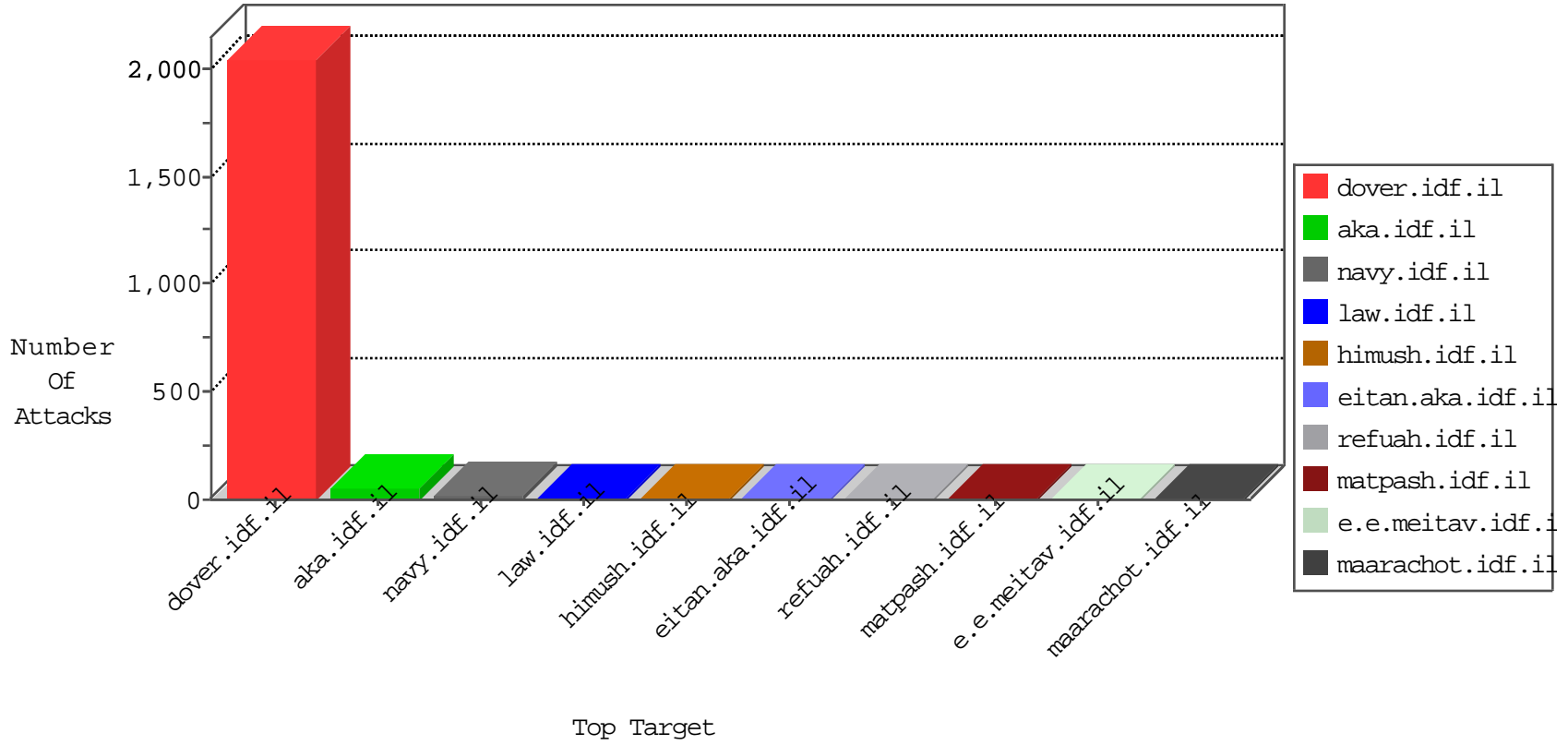


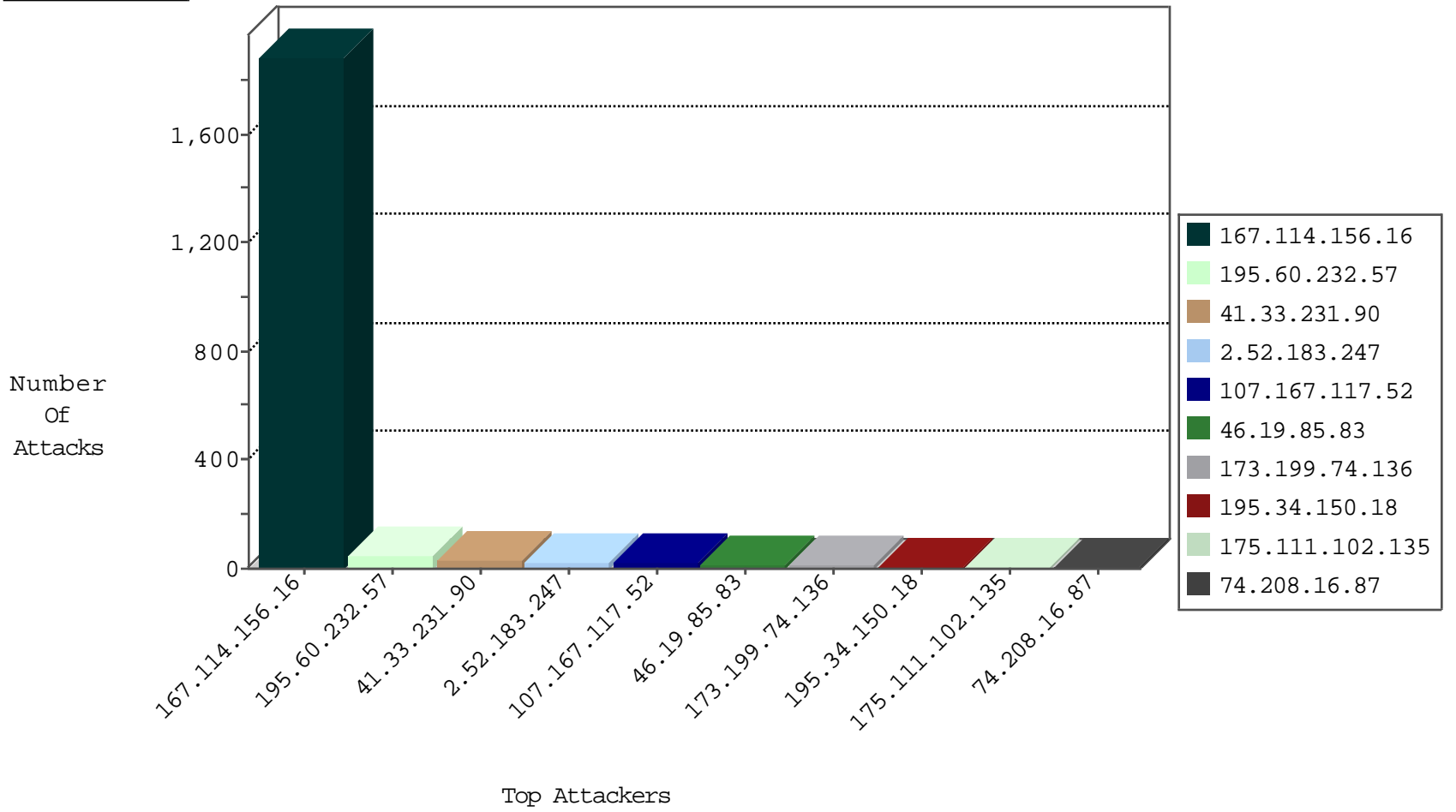
IDF Under Attack Daily Report



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	3184
89.248.174.4	Netherlands	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
141.212.122.199	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
71.6.165.200	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
208.67.1.60	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1

01-07-2016-03:04:07 to 01-07-2016-04:04:07

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
66.249.73.214	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
173.199.74.136	147.237.77.227	United Kingdom	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.199.74.136	147.237.77.74	United Kingdom	law.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.199.74.136	147.237.76.38	United Kingdom	e.e.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.199.74.136	147.237.8.46	United Kingdom	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.199.74.136	147.237.0.200	United Kingdom	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
168.62.238.153	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.195.114	147.237.77.205	Russian Federation	prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
31.184.195.114	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.199.74.136	147.237.77.212	United Kingdom	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.199.74.136	147.237.76.197	United Kingdom	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.199.74.136	147.237.8.50	United Kingdom	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.199.74.136	147.237.8.27	United Kingdom	e.madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.199.74.136	147.237.0.35	United Kingdom	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
168.62.238.153	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
58.101.85.198	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.195.114	147.237.76.202	Russian Federation	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	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	30
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	27
107.167.117.52	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
2.52.183.247	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
195.60.232.57	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
175.111.102.135	New Zealand	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.85.83	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.83	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
199.30.24.99	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
94.230.86.242	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.65.163.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
207.46.13.152	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
2.52.183.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	2
204.79.180.27	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
2.52.183.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
182.69.49.192	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.52.183.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
207.46.13.152	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
65.181.118.10	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
5.213.33.31	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.130.5.231		147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	1
84.110.84.61	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
195.60.232.57	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
193.105.134.220	Sweden	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.112	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
108.61.123.66	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
208.115.111.68	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
71.62.91.187	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
195.60.232.57	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.26.146.172	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.130.5.231		147.237.76.196	e.sviva.idf.il	drop	SAM rule	drop	1
178.17.174.99	Moldova, Republic of	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
193.105.134.220	Sweden	147.237.0.33	idf.il	drop		drop	1
184.105.247.215	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.88	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
79.177.161.89	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
37.26.149.234	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
185.130.5.231		147.237.77.74	law.idf.il	drop	SAM rule	drop	1
178.62.2.87	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
104.33.214.83	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
193.105.134.220	Sweden	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.102.253.45	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.239	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.90	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
84.110.84.61	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
37.26.149.234	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
188.143.232.16	Russian Federation	147.237.77.74	law.idf.il	drop	SAM rule	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
74.208.16.87	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 74.208.16.87	Block	5
77.125.122.176	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
80.246.136.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
174.17.188.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	2
84.111.187.38	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
74.208.16.87	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
66.249.64.191	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/1/1381.pdf	Block	1
185.25.151.159	Poland	147.237.72.156	aman.idf.il	Unauthorized URL Access to testp3.pospr.waw.pl/testproxy.php	Block	1
91.228.196.139	Poland	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
66.249.69.38	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1770	Block	1
207.46.13.123	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/123rf-phone-ajax.php	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
66.249.66.26	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1400-he/atal.aspx	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
91.228.196.139	Poland	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-signup.php	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1927-he/cogat.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
157.55.39.107	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/sip_storage/files/6/1446.pdf/	Block	1
77.247.181.162	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.66.29	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	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
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
68.180.230.240	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/2/112922.pdf×ž x x" x™x' x•xª	Block	1
50.200.126.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
162.203.2.233	United States	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/gyus/authenticationservice.asmx/getauthuser	Block	1
66.249.66.131	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/2934.pdf	Block	1
207.46.13.85	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	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
65.181.118.10	United States	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
66.249.66.191	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
207.46.13.123	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1