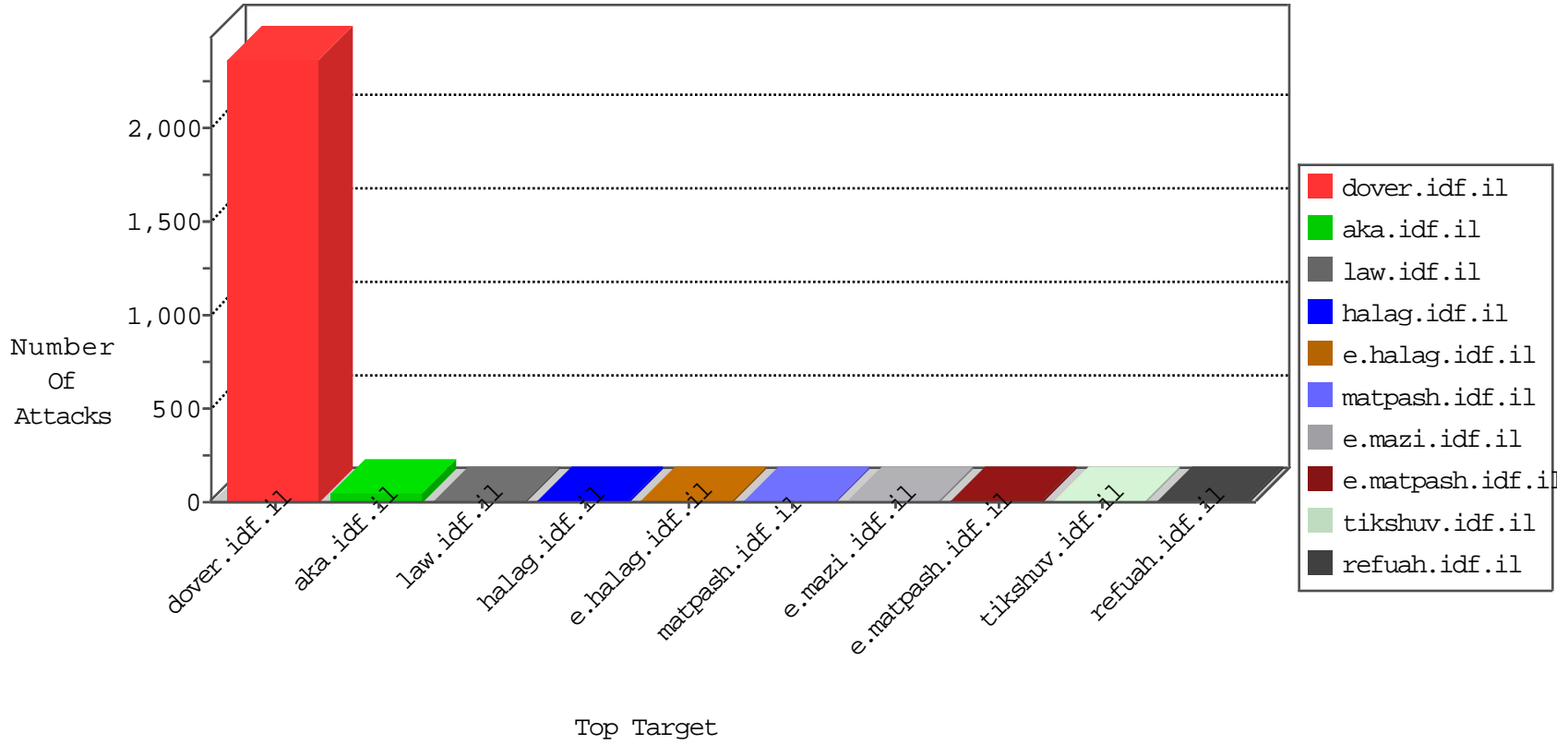


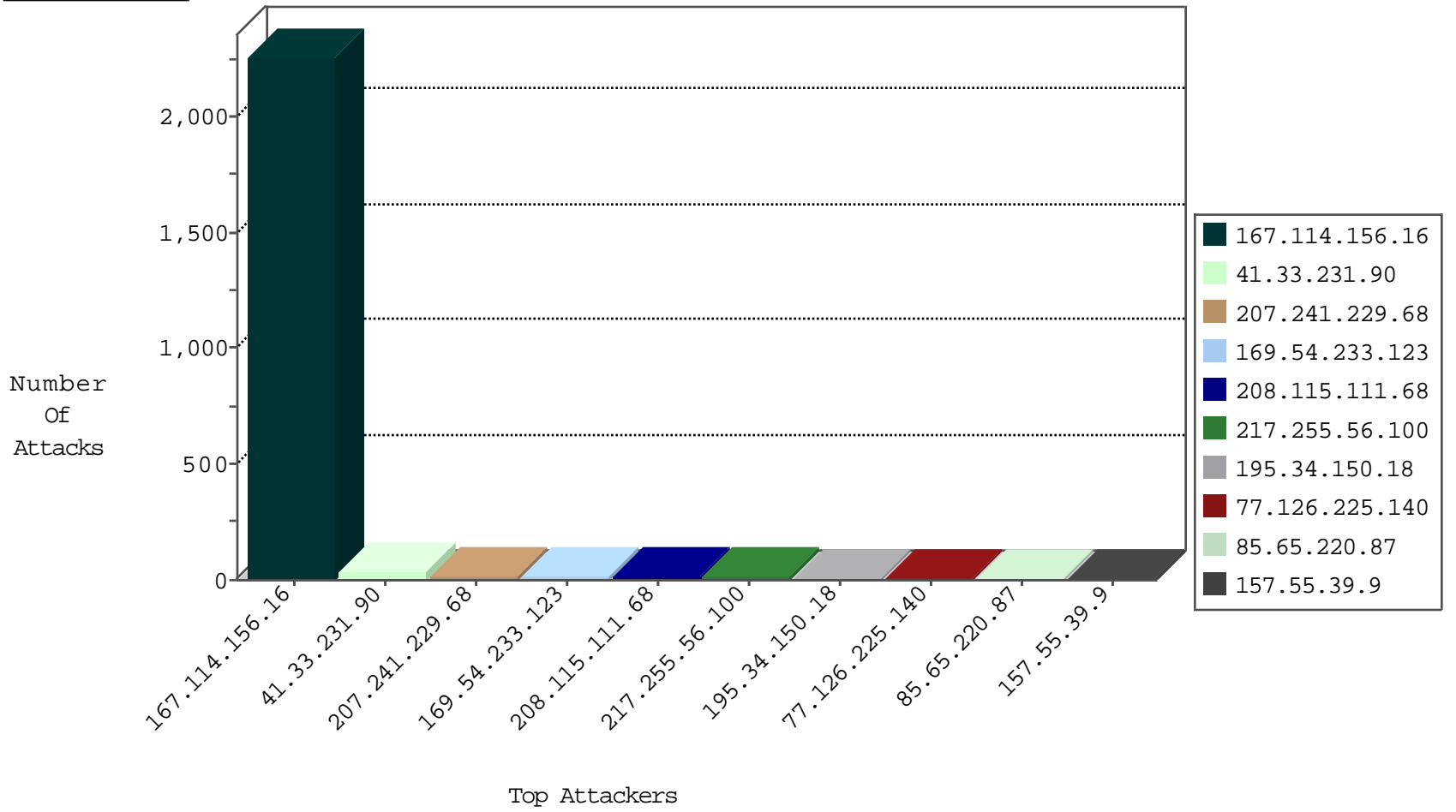
IDF Under Attack Daily Report



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

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
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
98.119.105.221	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
98.119.105.221	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
169.54.233.123	147.237.77.234	Netherlands	halag.idf.il	ET SCAN Potential SSH Scan	1
88.249.106.23	147.237.76.39	Turkey	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.233.123	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 2048	1
169.54.233.123	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -f -sS	1
169.54.233.123	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.123	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.123	147.237.76.30	Netherlands	himush.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.123	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
98.119.105.221	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.0.200	Ukraine	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.233.123	147.237.77.226	Netherlands	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.123	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.233.123	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
5.39.222.253	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
169.54.233.123	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.123	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN Potential SSH Scan	1
169.54.233.123	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	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	34
207.241.229.68	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
217.255.56.100	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
208.115.111.68	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	10
77.126.225.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.9	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
207.46.13.169	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	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
157.55.39.194	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.65.220.87	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.183	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
208.115.111.73	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
176.12.139.77	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
85.65.220.87	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
198.20.69.74	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.175.193.164	Germany	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
104.128.144.131	Canada	147.237.77.226	www.chamatz.aka.idf.il	drop	SAM rule	drop	1
74.82.47.35	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.4.109.148	Germany	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.116	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
146.185.239.102	Russian Federation	147.237.76.148	ggcenter.aka.idf.il	drop		drop	1
85.65.220.87	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.103	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
198.20.69.98	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
115.230.124.164	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.40	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
208.115.111.73	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
46.4.109.148	Germany	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.212	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
149.210.150.83	Netherlands	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
85.65.220.87	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
74.82.47.14	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.13.2.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
115.239.228.99	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
46.4.109.148	Germany	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
98.234.222.114	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
74.82.47.15	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.103	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
118.193.177.100	China	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
212.106.77.124	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
46.4.109.148	Germany	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
195.66.76.4	Germany	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
98.234.222.114	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.32	United States	147.237.0.19	madim.atal.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
91.207.158.134	Norway	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 91.207.158.134	Block	5
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	2
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	2
157.55.39.194	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
40.77.167.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
157.55.39.85	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/i/js_inst	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
2.54.29.92	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 2.54.29.92	None	1
176.13.22.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	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
40.77.167.105	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
157.55.39.111	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8924-he/refuah.aspx	Block	1
37.26.149.143	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
176.13.22.136	Israel	147.237.77.234	halag.idf.il	PHP Attempt	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
64.19.78.242	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
207.46.13.59	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
37.142.64.15	Israel	147.237.76.147	chinuch.aka.idf.il	PHP Attempt	Block	1
176.13.22.136	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/xmlrpc.php	Block	1
118.193.177.100	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.69.77	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/sitemap/sitemap.aspx	Block	1
207.46.13.169	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.206	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/i/related_users/2382841945	Block	1
91.207.158.134	Norway	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
37.142.64.15	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/xmlrpc.php	Block	1
184.105.139.68	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
131.253.25.199	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/i/jot	Block	1
66.249.78.111	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
2.54.29.92	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	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
176.13.22.136	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1