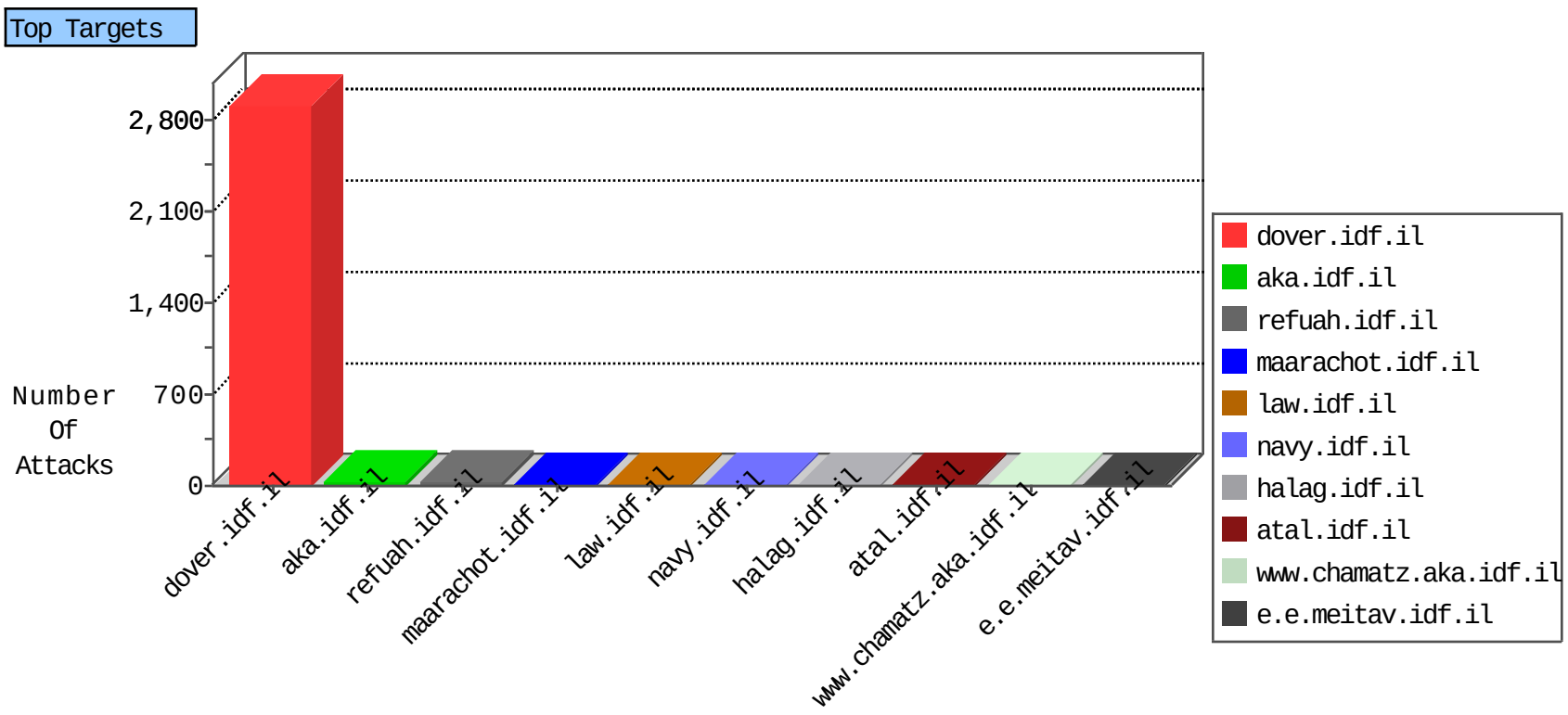
12-04-2015-04:04:04 to 12-04-2015-05:04:04

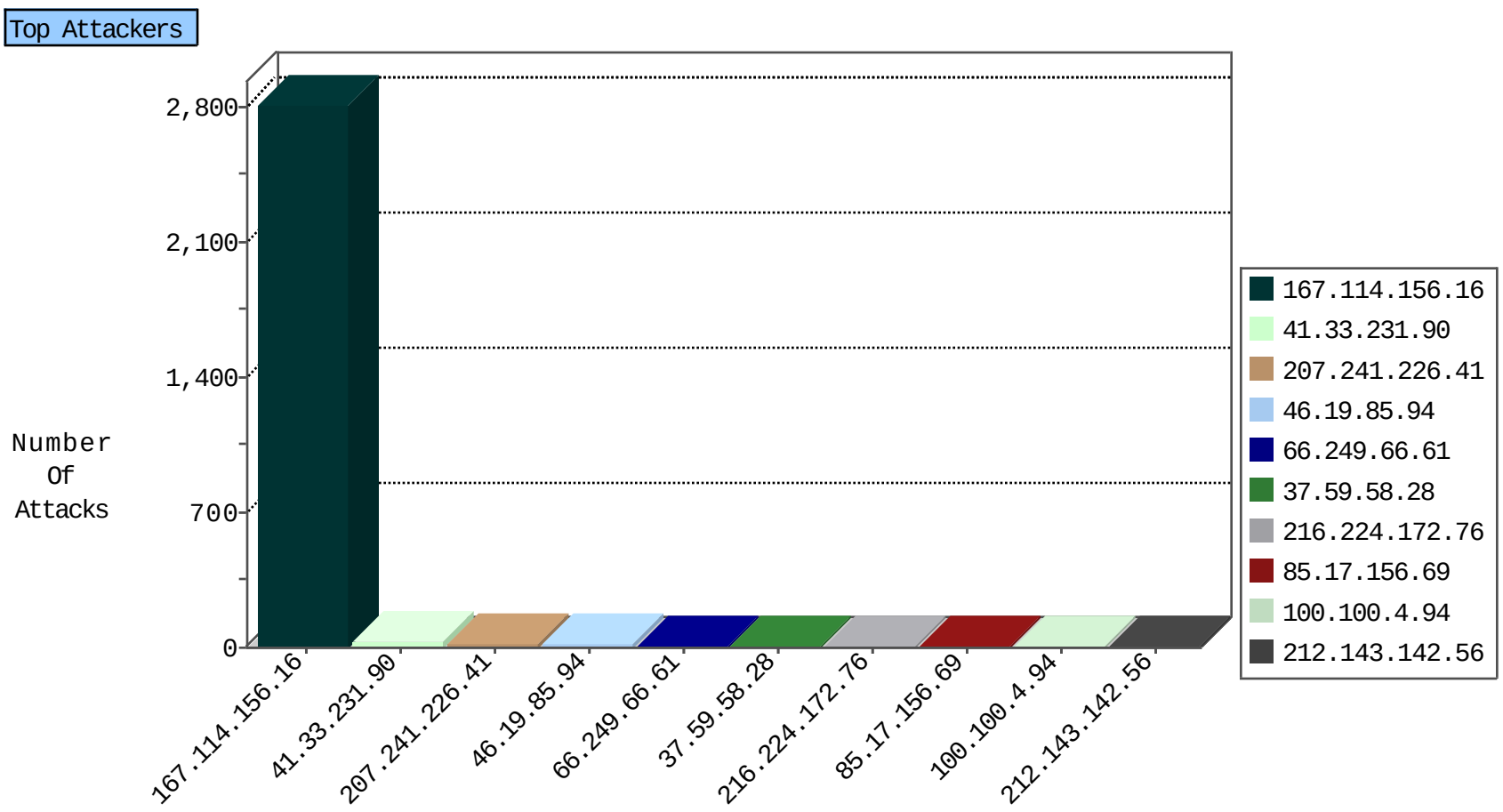
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

12-04-2015-04:04:04 to 12-04-2015-05:04:04

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	3403
204.42.253.2	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	2

12-04-2015-04:04:04 to 12-04-2015-05:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-04-2015-04:04:04 to 12-04-2015-05:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
85.17.156.69	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
182.254.149.138	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
114.247.172.61	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 2048	1
94.102.48.195	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
85.17.156.69	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential SSH Scan	1
85.17.156.69	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
85.17.156.69	147.237.8.14	Netherlands	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
85.17.156.69	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.6.168.220	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
46.151.55.35	147.237.77.170	Ukraine	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
131.109.15.2	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
114.247.172.61	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -f -sS	1
94.102.48.195	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
85.17.156.69	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
85.17.156.69	147.237.72.156	Netherlands	aman.idf.il	ET SCAN Potential SSH Scan	1

12-04-2015-04:04:04 to 12-04-2015-05:04:04

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
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
100.100.4.94		147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.94	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.178.110.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.100.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.94	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
172.56.15.97	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	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
76.89.147.15	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.59.58.28	France	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
157.55.39.169	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.59.58.28	France	147.237.72.14	dover.idf.il(old)	drop	First packet isn't SYN	drop	2
37.59.58.28	France	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
141.212.122.117	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.255.253.188	Russian Federation	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.131	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
108.29.199.83	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.34	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.128	United States	147.237.76.148	gqcenter.aka.idf.i	drop		drop	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
141.212.122.133	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.34	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
37.130.227.133	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.129	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.134	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
115.230.124.164	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
74.82.47.42	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.130	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
107.201.165.186	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.59.58.28	France	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.143	United States	147.237.76.148	gqcenter.aka.idf.i	drop		drop	1
141.212.122.116	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.46	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.130	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
108.29.199.83	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
74.82.47.14	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
149.78.222.237	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

12-04-2015-04:04:04 to 12-04-2015-05:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.241.226.41	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 207.241.226.41	Block	13
207.241.226.41	United States	147.237.76.42	refuah.idf.il	PHP Attempt	Block	4
66.249.66.75	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.66.75	Block	3
216.224.172.76	United States	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	3
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	2
216.224.172.76	United States	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 216.224.172.76	Block	2
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	2
157.55.39.18	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/history/stm	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
213.57.49.202	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 4d9c6f40 in www.aka.idf.il/main/kapatz/contactus.aspx	None	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.255.215.87	Block	1
66.249.66.81	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/×©×§×•×¤×™×ª 3	Block	1
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
157.55.39.115	United States	147.237.72.166	aka.idf.il	Unknown Parameter 1225bd80 in www.aka.idf.il/iturim/asp/results.asp	None	1
82.166.240.204	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
216.224.172.76	United States	147.237.77.170	maarachot.idf.il	Multiple Admin Blocking from 216.224.172.76	Block	1
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter gt; in www.aka.idf.il/main/rabanut/general.aspx	None	1
199.59.148.211	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/6/size220x0/17646.jpg	Block	1
141.212.122.129	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to /x	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/ och http:/www.idfblog.com/	Block	1
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	1
207.241.226.41	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/templates/news/piwik.php	Block	1
157.55.39.243	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/sachar/klali.aspx	None	1
84.108.32.126	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
141.212.122.129	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to /x	Block	1
68.180.231.40	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/sip_storage/files/7/1437.pdf/	Block	1
66.249.66.26	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1235-he/atal.aspx	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
157.55.39.244	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/recruitlane.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
66.249.66.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/×©×§×•×¤×™×ª 2	Block	1
45.35.71.181		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
207.46.13.119	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
141.212.122.129	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to /x	Block	1
79.179.99.94	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
66.249.66.29	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1232-he/atal.aspx	Block	1
173.45.108.26	United States	147.237.77.226	www.chamatz.aka.idf.il	Admin Blocking	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
216.224.172.76	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.maarachot.idf.il/index.php	Block	1
66.249.66.75	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/about/_layouts/authenticate.aspx	Block	1
66.249.66.23	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1234-he/atal.aspx	Block	1

12-04-2015-04:04:04 to 12-04-2015-05:04:04