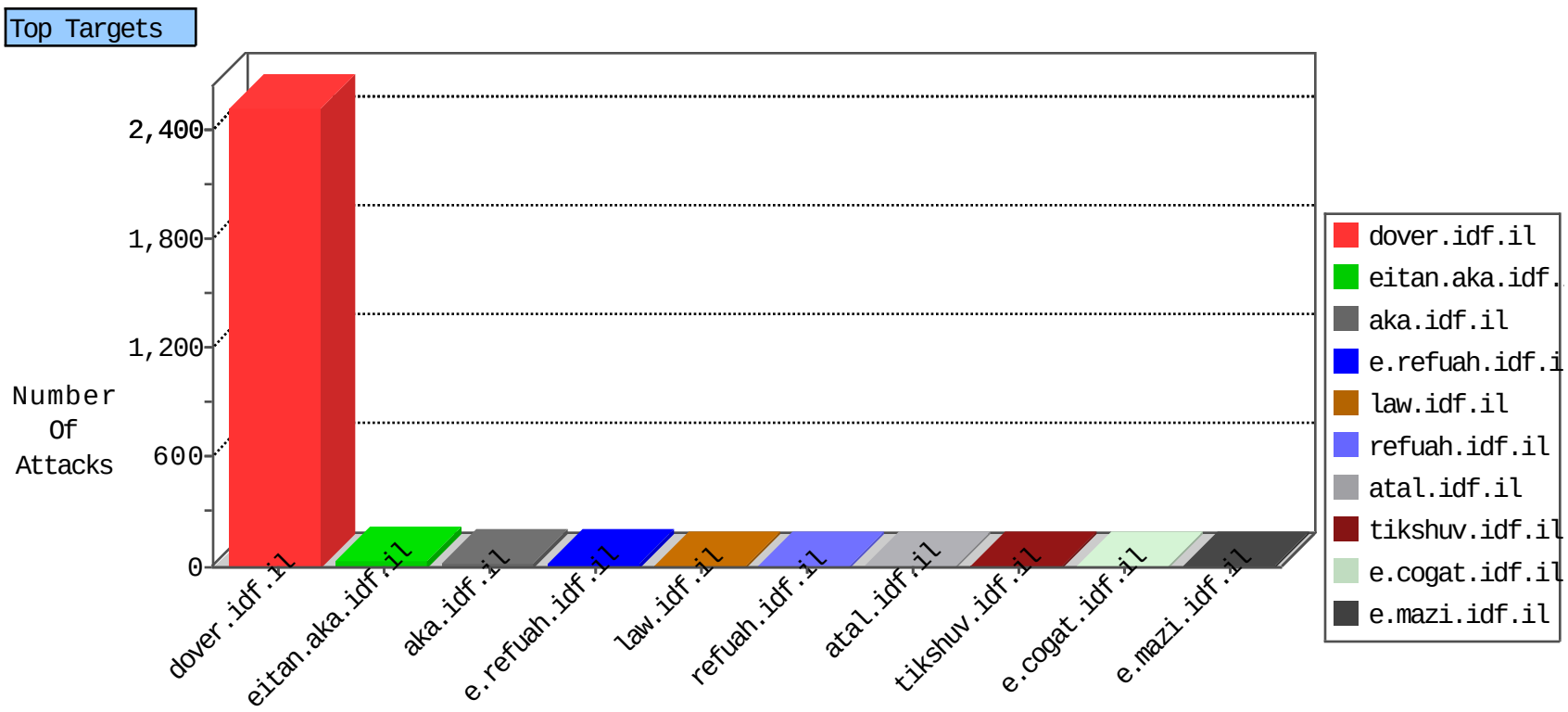
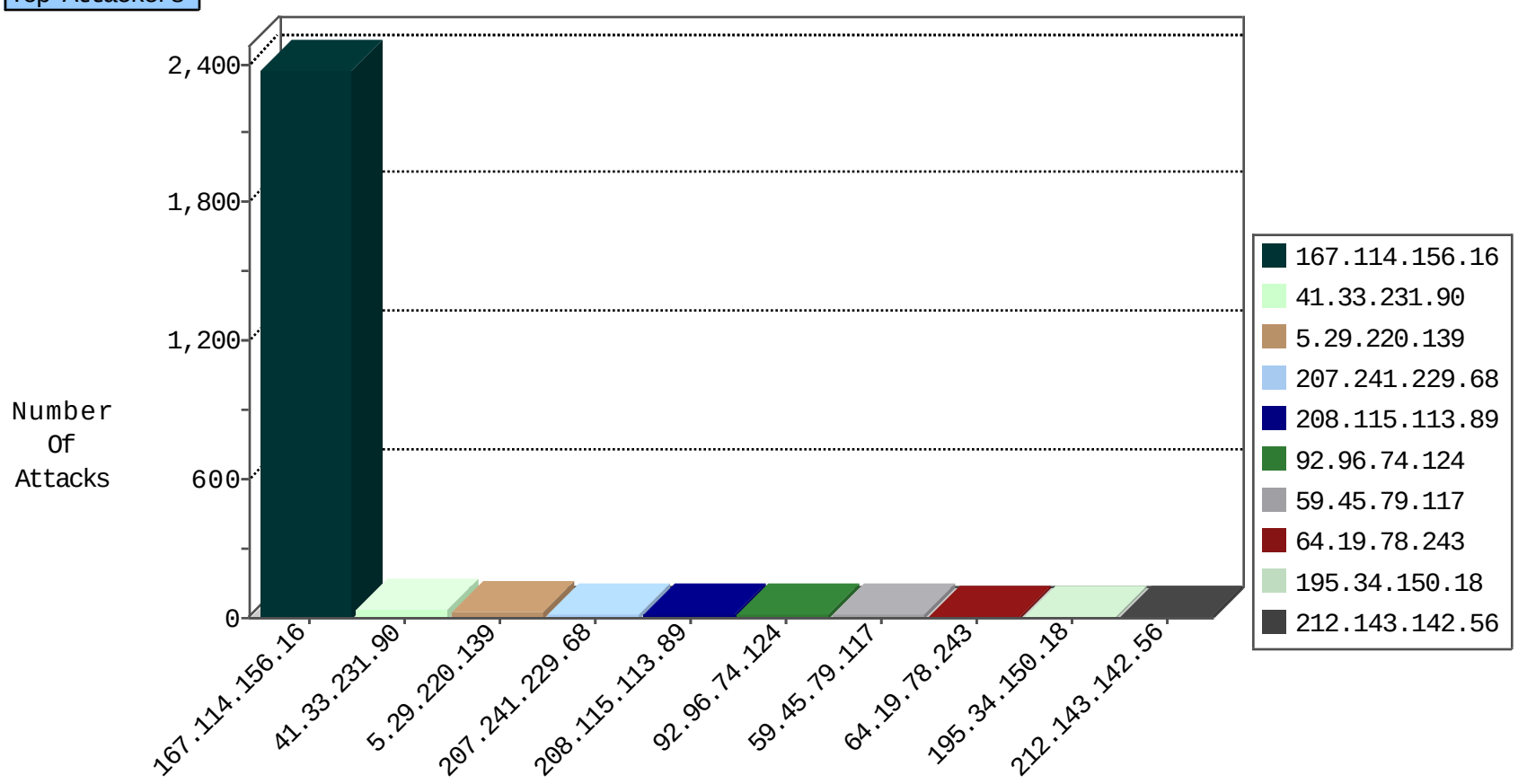
12-19-2015-04:04:03 to 12-19-2015-05:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-19-2015-04:04:03 to 12-19-2015-05:04:03

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	3429
134.147.203.115	Germany	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	2

12-19-2015-04:04:03 to 12-19-2015-05:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.154.191.97	France	147.237.77.216	dover.idf.il	19791: HTTP: WordPress N-Media PHP File Upload	Block	1

12-19-2015-04:04:03 to 12-19-2015-05:04:03

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
40.115.58.160	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
78.188.42.178	147.237.76.30	Turkey	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
196.47.173.21	147.237.77.179	Cote D'Ivoire	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
146.185.250.2	147.237.77.176	Russian Federation	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
146.185.250.2	147.237.76.31	Russian Federation	nakchal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
104.43.236.38	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
104.43.236.38	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
94.102.48.195	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	147.237.77.179	Cote D'Ivoire	e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
61.244.49.137	147.237.0.15	Hong Kong	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	147.237.77.179	Cote D'Ivoire	e.mazi.idf.il	ET SCAN NMAP -f -sS	1
59.45.79.117	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
146.185.250.2	147.237.77.212	Russian Federation	e.dover.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
146.185.250.2	147.237.77.61	Russian Federation	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
104.43.236.38	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 4096	1
59.45.79.117	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
104.43.236.38	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 4096	1
59.45.79.117	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
94.102.60.89	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.195	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1

12-19-2015-04:04:03 to 12-19-2015-05:04:03

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
207.241.229.68	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
64.19.78.243	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	10
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	SAM rule	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
208.115.113.89	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
130.207.203.56	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.29.220.139	Israel	147.237.76.200	eitan.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
92.96.74.124	United Arab Emirates	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
199.30.24.178	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
92.96.74.124	United Arab Emirates	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	3
172.56.35.62	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
212.117.180.21	Luxembourg	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
92.96.74.124	United Arab Emirates	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	2
208.115.111.73	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
208.115.113.89	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	2
187.107.218.79	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
92.96.74.124	United Arab Emirates	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
92.96.74.124	United Arab Emirates	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	2
93.115.95.204	Anonymous Proxy	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
212.47.238.193	France	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
77.237.138.51	Czech Republic	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
206.54.185.34	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
104.245.104.3		147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
74.82.47.28	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
193.90.12.90	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
158.69.208.131	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
93.115.95.216	Anonymous Proxy	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
77.244.254.230	Austria	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
46.45.137.71	Turkey	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
184.105.139.104	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
110.210.20.210	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
208.115.113.89	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
74.82.47.31	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
94.242.246.23	Luxembourg	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
77.247.181.165	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
184.105.247.224	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.48	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
198.20.69.74	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
37.187.129.166	France	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
171.25.193.20	Sweden	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
95.211.210.112	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
216.218.206.76	United States	147.237.77.61	e.cogat.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
85.24.215.117	Sweden	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
208.115.111.73	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
72.52.75.27	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1

12-19-2015-04:04:03 to 12-19-2015-05:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.220.139	Israel	147.237.76.200	eitan.aka.idf.i	Too Many of the Same Response Code (404) in Session from 5.29.220.139	Block	23
204.13.200.200	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 204.13.200.200	Block	2
77.49.81.205	Greece	147.237.77.74	law.idf.il	PHP Attempt	Block	2
46.19.86.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
195.154.191.97	France	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
49.204.21.225	India	147.237.76.200	eitan.aka.idf.i	Unauthorized URL Access to www.eitan.aka.idf.il/xmlrpc.php	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
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
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2110-he/cogat.aspx	Block	1
5.22.129.144	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
195.154.191.97	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-admin/admin-ajax.php	Block	1
77.244.254.230	Austria	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
66.249.69.81	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1236-he/atal.aspx	Block	1
216.218.207.138	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
110.210.20.210	China	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
77.49.81.205	Greece	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 77.49.81.205	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
66.249.69.89	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1224-he/atal.aspx	Block	1
195.154.191.97	France	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
207.46.13.131	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1608-15309-he/upload_pic.html	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
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
195.154.191.97	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 195.154.191.97	Block	1
77.49.81.205	Greece	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
49.204.21.225	India	147.237.76.200	eitan.aka.idf.i	PHP Attempt	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
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
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/tfasim.aspx	Block	1
77.237.138.51	Czech Republic	147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	1

12-19-2015-04:04:03 to 12-19-2015-05:04:03