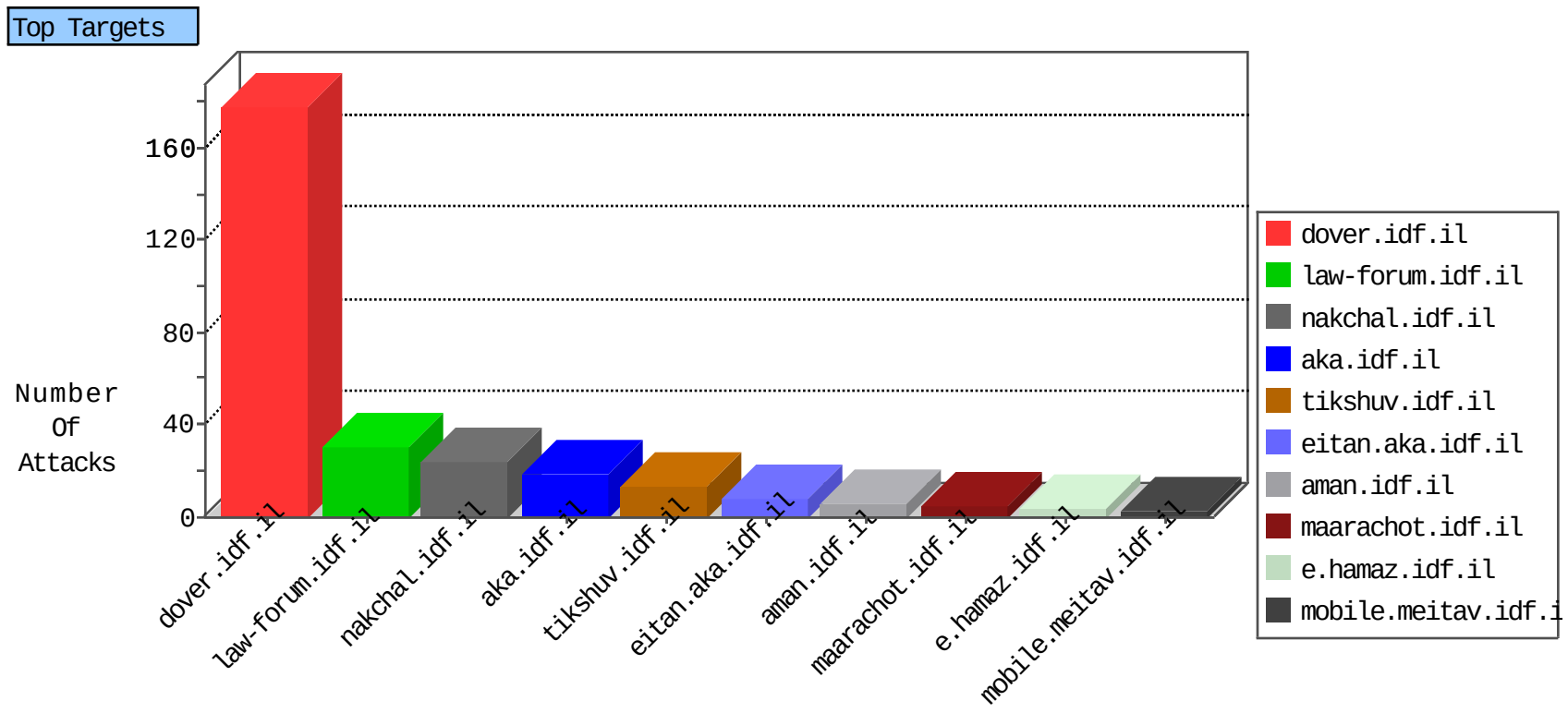
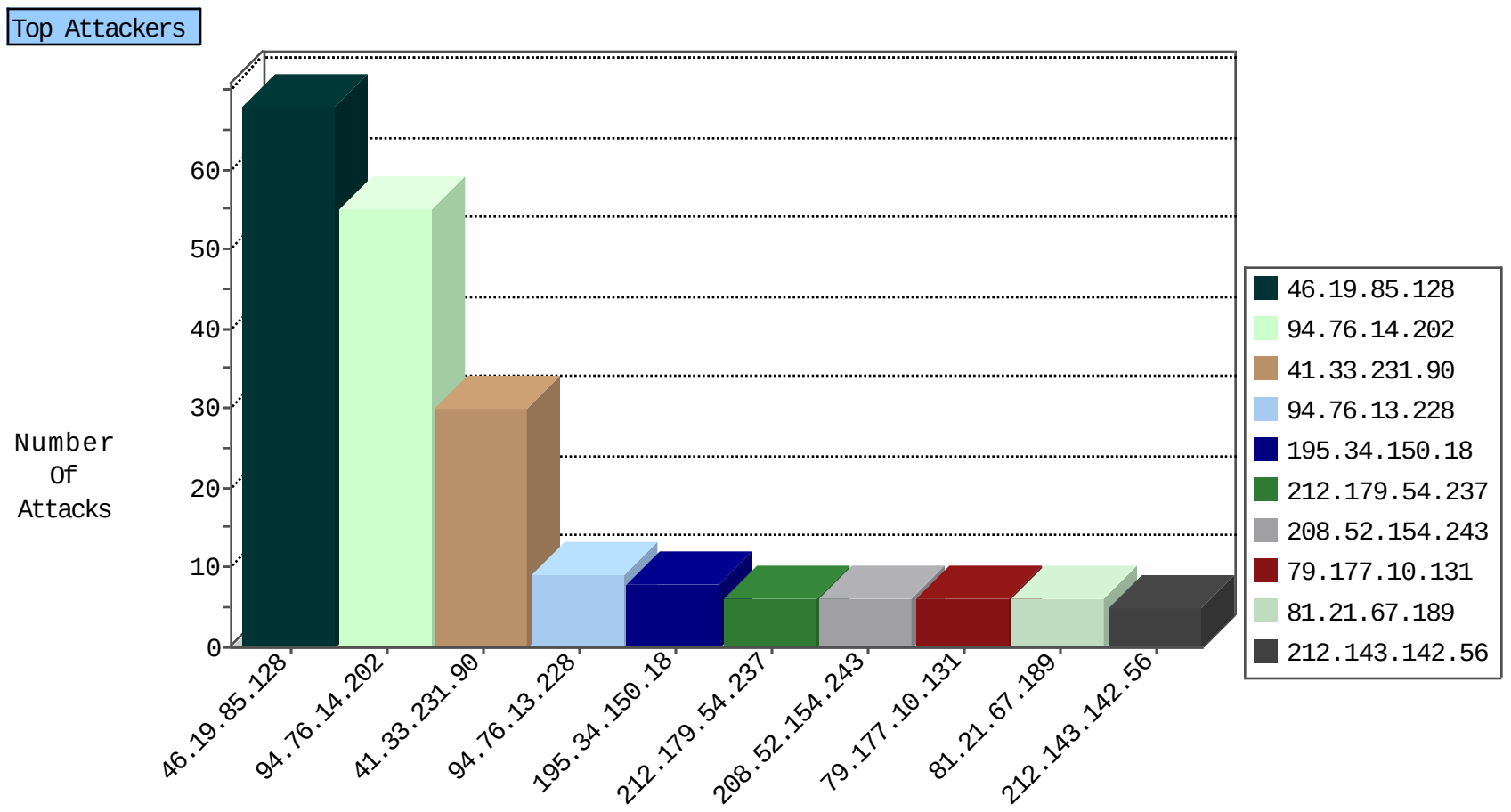
01-28-2016-03:04:05 to 01-28-2016-04:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-28-2016-03:04:05 to 01-28-2016-04:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
94.76.13.228	Bahrain	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
94.76.13.228	Bahrain	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
167.114.92.57	Canada	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
89.248.160.138	Netherlands	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1

01-28-2016-03:04:05 to 01-28-2016-04:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
202.69.240.159	Hong Kong	147.237.77.170	maarachot.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	4
94.76.13.228	Bahrain	147.237.0.34	tikshuv.idf.il	C107: DDOS-Spoofed HTTP Packets	Block	2
46.119.121.146	Ukraine	147.237.76.200	eitan.aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1

01-28-2016-03:04:05 to 01-28-2016-04:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.19.85.128	147.237.77.216	Israel	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	48
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
94.76.11.99	147.237.0.34	Bahrain	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	2
66.249.78.157	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.78.44	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
81.21.67.189	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	2
94.76.13.228	147.237.76.38	Bahrain	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -sS window 1024	1
46.161.40.120	147.237.76.198	Russian Federation	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
199.180.114.67	147.237.72.167	Poland	ishurim.aka.idf.il	ET SCAN NMAP -f -sS	1
177.43.249.41	147.237.76.39	Brazil	mobile.meitav.idf.i	ET SCAN NMAP -sS window 4096	1
113.171.23.126	147.237.77.170	Vietnam	maarachot.idf.il	ET SCAN Potential SSH Scan	1
113.171.23.126	147.237.0.35	Vietnam	akaws.idf.il	ET SCAN Potential SSH Scan	1
94.76.13.228	147.237.0.34	Bahrain	tikshuv.idf.il	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	1
66.249.78.81	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
66.240.213.93	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
199.180.114.67	147.237.72.167	Poland	ishurim.aka.idf.il	ET SCAN NMAP -sS window 2048	1
177.43.249.41	147.237.76.39	Brazil	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
113.171.23.126	147.237.76.177	Vietnam	ncore.idf.il	ET SCAN Potential SSH Scan	1

01-28-2016-03:04:05 to 01-28-2016-04:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
94.76.14.202	Bahrain	147.237.77.19	law-forum.idf.il	drop	SAM rule	drop	31
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
94.76.14.202	Bahrain	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	24
46.19.85.128	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
79.177.10.131	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
46.19.85.195	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
69.124.41.84	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
187.189.195.40	Mexico	147.237.77.227	e.hamaz.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
99.224.136.34	Canada	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
208.52.154.243	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
84.228.202.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.76.13.228	Bahrain	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	2
31.210.187.85	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
172.56.6.152	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.85.128	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
40.77.167.69	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.128	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Urgent Data Enforcement	TCP segment with urgent pointer (no data). Urgent data indication was stripped. Please refer to sk36869.	alert	2
208.115.113.89	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
46.19.85.128	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Urgent Data Enforcement	TCP segment with urgent pointer (no data). Urgent data indication was stripped. Please refer to sk36869.	drop	2
216.218.206.100	United States	147.237.0.33	idf.il	drop		drop	1
31.210.186.142	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
208.52.154.243	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
81.169.237.146	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
187.44.116.226	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
220.181.108.162	China	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
208.52.154.243	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
81.169.237.146	Germany	147.237.76.38	e.e.meitav.idf.i	drop	SAM rule	drop	1
187.44.116.226	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
220.181.108.162	China	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
176.77.29.102	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
81.169.237.146	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	1
213.57.194.37	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
178.191.248.1	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
213.57.194.37	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
2.52.32.11	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
81.169.237.146	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	1
208.115.113.89	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
178.191.248.1	Austria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
89.138.193.111	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

01-28-2016-03:04:05 to 01-28-2016-04:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.21.67.189	United Kingdom	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
197.38.206.55	Egypt	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
197.38.206.55	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	2
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19916-he/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
37.142.68.103	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
113.66.40.84	China	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/592-6584-en/patzar.aspx/trackback/	Block	1
66.249.78.234	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
46.119.121.146	Ukraine	147.237.76.200	eitan.aka.idf.i	Unauthorized URL Access to www.eitan.aka.idf.il/wp-login.php	Block	1
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
85.25.103.12	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
37.187.129.166	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
150.70.173.46	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
54.145.198.46	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
207.46.13.20	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
94.76.13.228	Bahrain	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/robots.txt	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
40.77.167.67	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
150.70.173.46	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.64.75	Israel	147.237.76.200	eitan.aka.idf.i	Unauthorized URL Access to www.eitan.aka.idf.il/templates/general/general.aspx	Block	1
207.46.13.49	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
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
66.249.78.228	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.228	Block	1
40.77.167.91	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list.htm	Block	1
81.21.67.189	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
66.249.78.81	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
208.52.154.243	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to /dbadmin/scripts/setup.php	Block	1
2.54.27.197	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.78.228	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_pictures.asp	Block	1
46.119.121.146	Ukraine	147.237.76.200	eitan.aka.idf.i	PHP Attempt	Block	1
81.21.67.189	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-10890-en/xmlrpc.php	Block	1

01-28-2016-03:04:05 to 01-28-2016-04:04:05