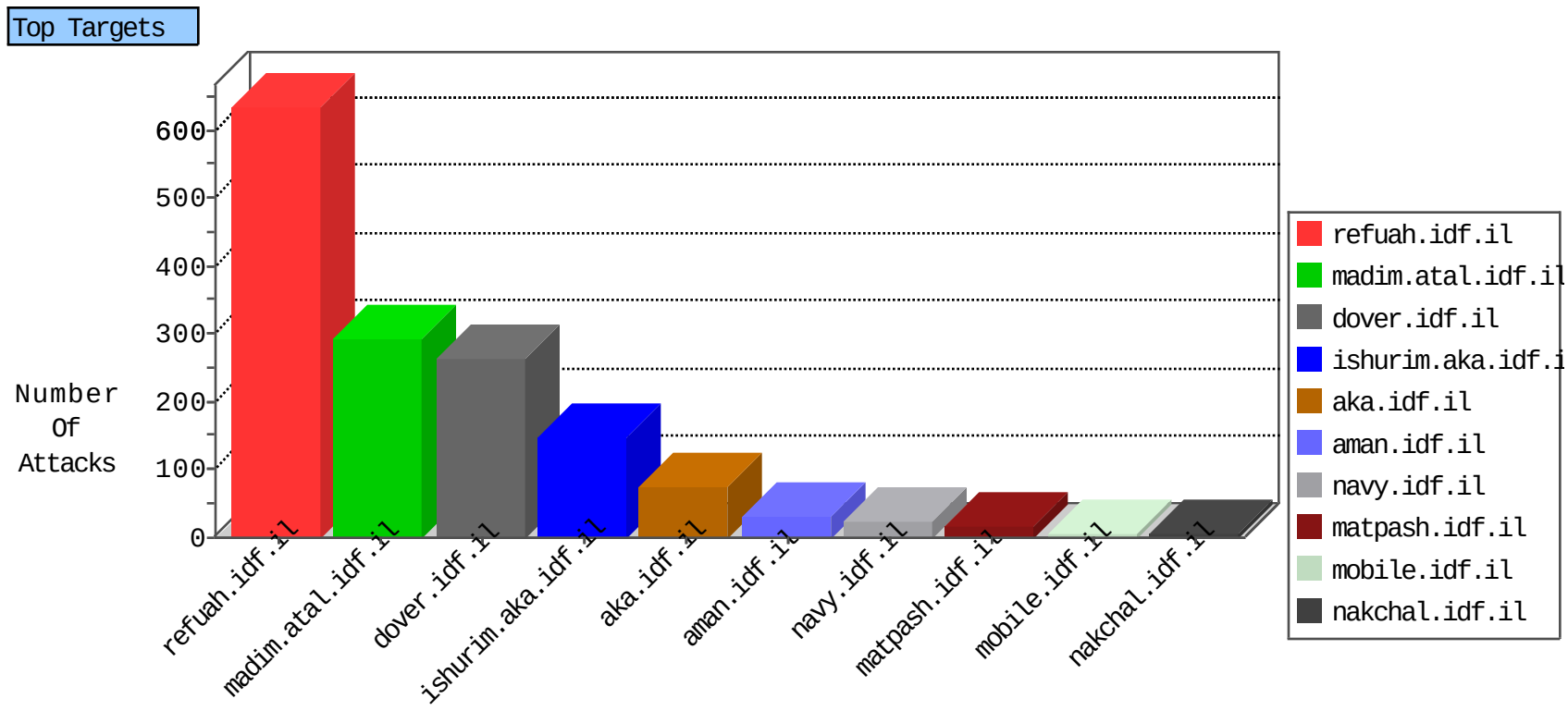
10-02-2016-20:04:07 to 10-02-2016-21:04:07

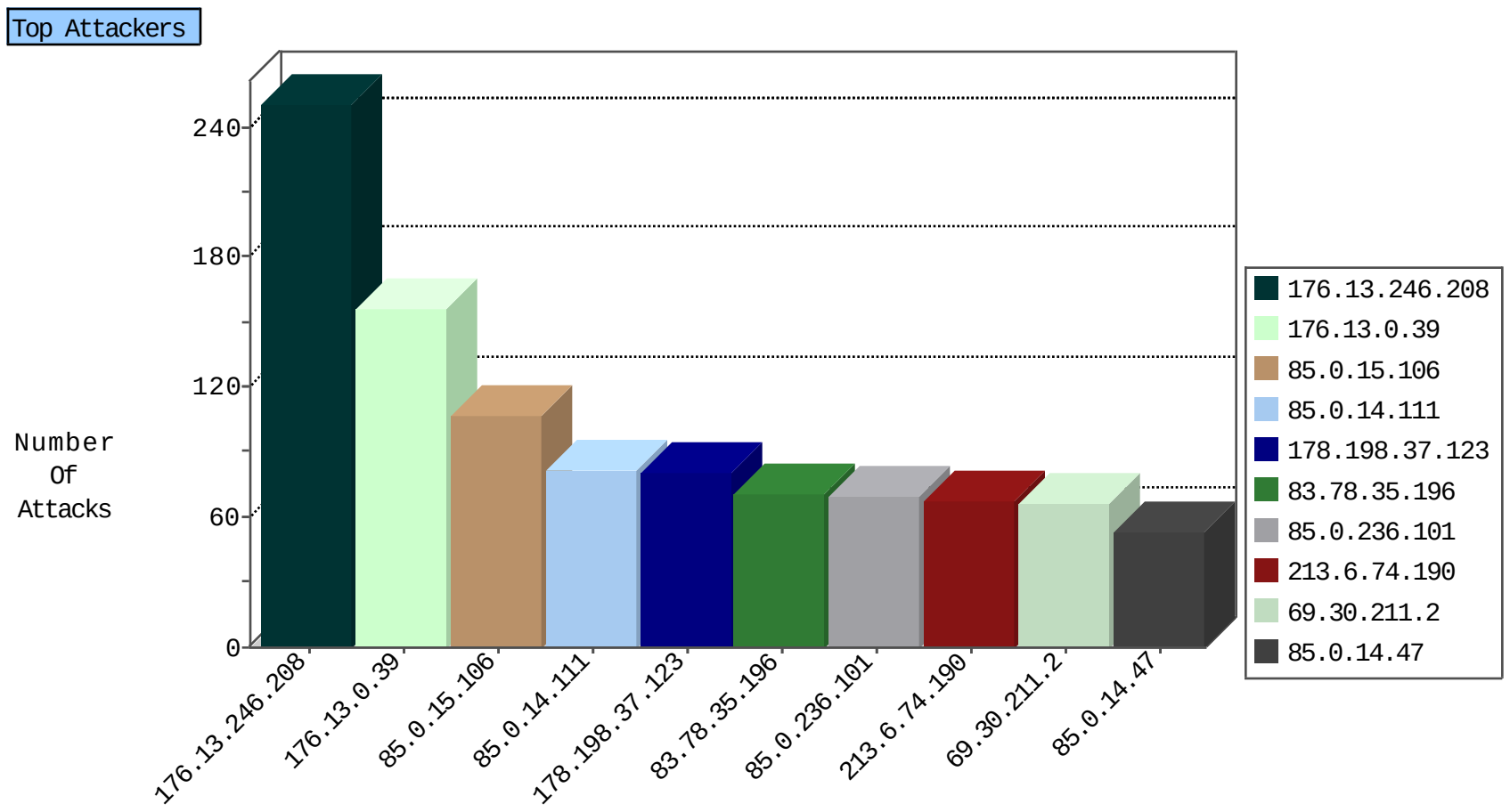
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

10-02-2016-20:04:07 to 10-02-2016-21:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
194.177.16.3	Israel	147.237.76.86	navy.idf.il	Black List	drop	3
141.212.122.90	United States	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
180.97.106.161	China	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1

10-02-2016-20:04:07 to 10-02-2016-21:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.211.2	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	58
69.30.211.2	United States	147.237.76.31	nakchal.idf.il	C1000074: HTTP: majestic bot	Permit	4
69.30.211.2	United States	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	3

10-02-2016-20:04:07 to 10-02-2016-21:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
146.200.148.0	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	3
91.121.135.78	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	3
208.100.26.228	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	2
112.254.142.90	147.237.0.200	China	m4u.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.50	147.237.76.39	Ukraine	mobile.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
222.101.6.122	147.237.77.216	Korea, Republic of	dover.idf.il	WEB-FRONTPAGE /_vti_bin/ access	1
91.201.236.50	147.237.76.39	Ukraine	mobile.meitav.idf.il	ET SCAN NMAP -f -sS	1
208.100.26.228	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
79.180.99.224	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
58.220.2.5	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
187.11.196.145	147.237.72.14	Brazil	dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1
185.40.4.208	147.237.77.235	Russian Federation	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
185.40.4.208	147.237.77.226	Russian Federation	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
110.159.32.84	147.237.76.31	Malaysia	nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.50	147.237.76.39	Ukraine	mobile.meitav.idf.il	ET SCAN NMAP -sS window 2048	1
208.100.26.228	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.76.117	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
197.45.132.217	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.98	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
187.11.196.145	147.237.72.14	Brazil	dover.idf.il(old)	ET SCAN NMAP -f -sS	1
185.40.4.208	147.237.77.227	Russian Federation	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
185.40.4.208	147.237.77.212	Russian Federation	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1

10-02-2016-20:04:07 to 10-02-2016-21:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
213.6.74.190	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	68
176.13.0.39	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	38
176.13.0.39	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	38
176.13.0.39	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	33
176.13.0.39	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	26
85.0.15.106	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	23
107.167.112.52	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	23
85.0.15.106	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	22
85.0.15.106	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	22
85.0.15.106	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	22
85.0.15.106	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
85.0.14.111	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	18
85.0.14.111	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	17
178.198.37.123	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
178.198.37.123	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
178.198.37.123	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
178.198.37.123	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	16
85.0.14.111	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	16
83.78.35.196	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	16
83.78.35.196	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
83.78.35.196	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	15
85.0.236.101	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	15
178.198.37.123	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	15
178.198.37.123	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	15
85.0.236.101	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
85.0.14.111	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
83.78.35.196	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	14
85.0.236.101	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	14
85.0.236.101	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	14
85.0.14.47	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	13
46.19.85.233	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
85.0.236.101	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
85.0.14.47	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
46.19.85.233	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
85.0.14.47	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	12
39.40.157.144	Pakistan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
85.0.14.47	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	11
83.78.35.196	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
52.3.127.144	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	10
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
149.56.27.31	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
37.26.147.170	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
37.34.80.102	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.0.39	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.232	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.86.203	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
24.4.50.221	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
83.222.97.147	Russian Federation	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5

10-02-2016-20:04:07 to 10-02-2016-21:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.246.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	251
109.64.175.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
79.178.13.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
77.139.1.184	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.1.184	Block	3
217.132.148.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.48.13.17	Czech Republic	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/	Block	2
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.51	Block	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.76.81	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
212.199.144.158	Israel	147.237.76.200	eitan.aka.idf.il	PHP Attempt	Block	1
87.69.222.132	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 87.69.222.132 (Open Mode)	None	1
66.249.65.59	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8910-he/refuah.aspx	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
77.138.103.48	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
62.32.68.83	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
212.199.144.158	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/wp-login.php	Block	1
87.69.222.132	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.75.48	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/993/patzar.aspx	Block	1
66.102.9.22	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on aka.idf.il/main/home/default.aspx	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/fund/funddesc.asp	Block	1
180.76.15.28	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9836-he/refuah.aspx	Block	1
77.139.1.184	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/miyun/miyunderugtafkidim.aspx	Block	1
66.249.64.15	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
139.162.13.205	Singapore	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.76.76	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
2.55.11.23	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
206.253.226.23	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1

10-02-2016-20:04:07 to 10-02-2016-21:04:07