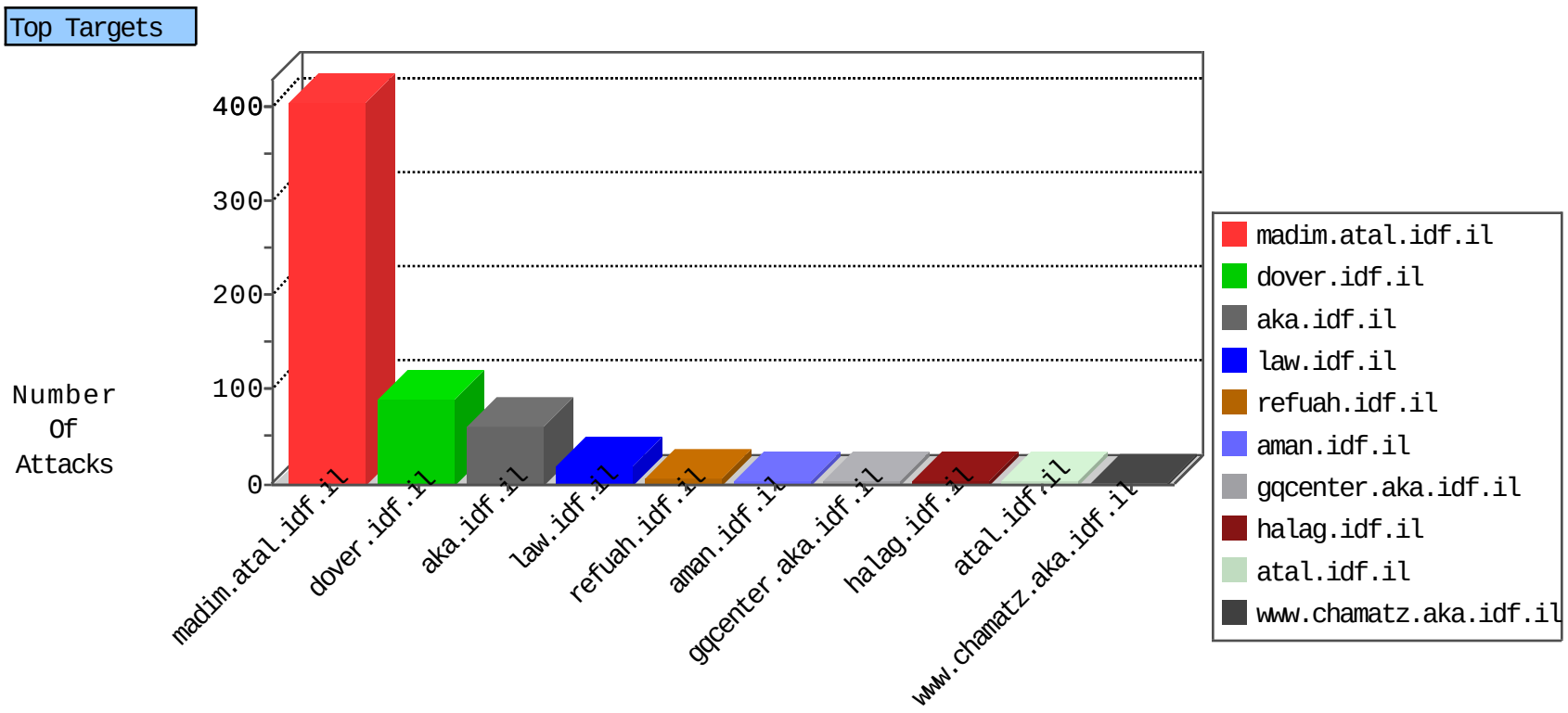
08-29-2016-13:04:06 to 08-29-2016-14:04:06

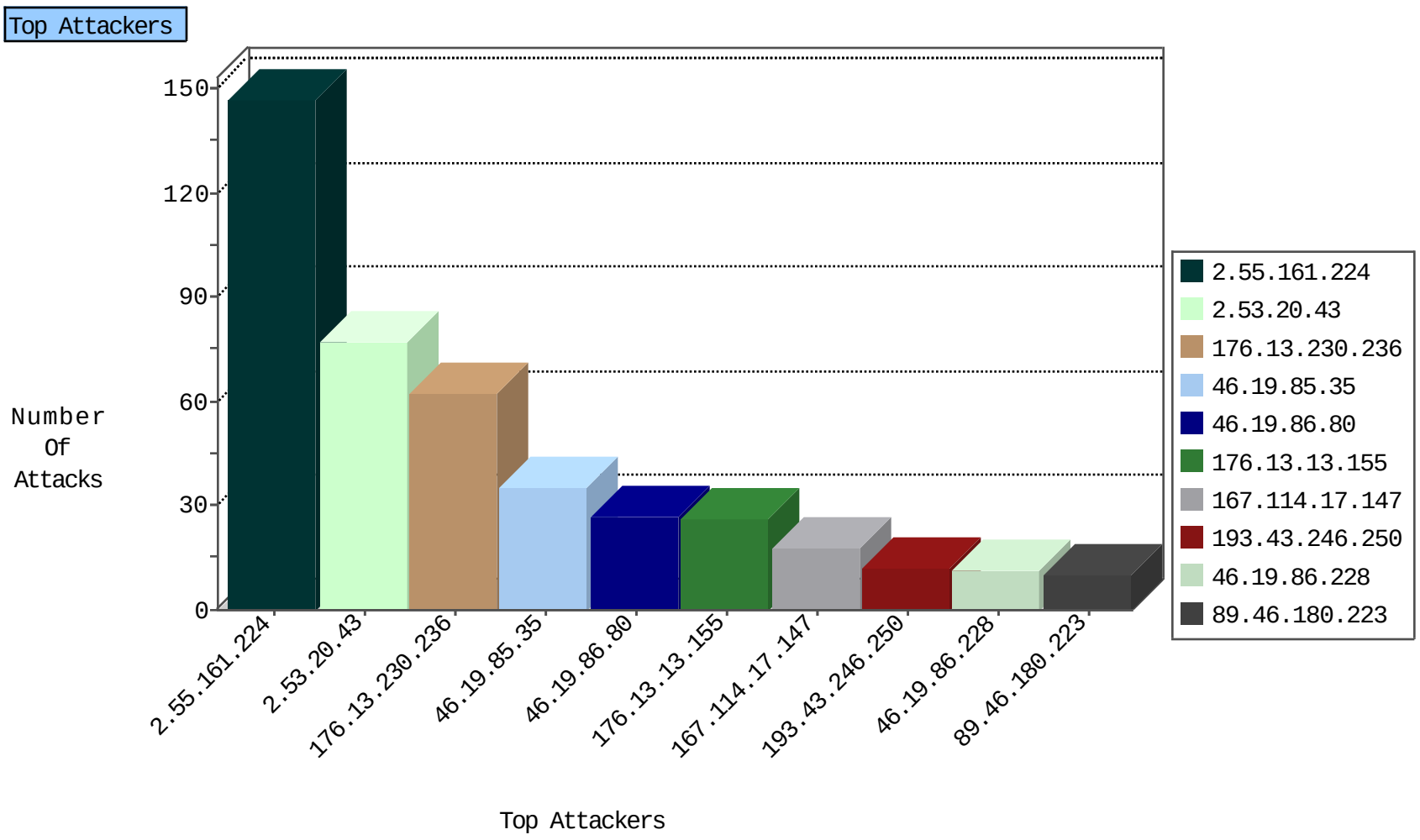
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

08-29-2016-13:04:06 to 08-29-2016-14:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.61.201	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4
82.80.78.2	Israel	147.237.77.226	www.chamatz.aka.idf.il	Black List	drop	2
185.94.111.1	Russian Federation	147.237.76.201	e.atal.idf.il	Black List	drop	1
71.6.158.166	United States	147.237.76.197	e.himush.idf.il	Black List	drop	1
209.126.136.2	United States	147.237.76.86	navy.idf.il	Black List	drop	1
109.65.142.86	Israel	147.237.72.166	aka.idf.il	Black List	drop	1

08-29-2016-13:04:06 to 08-29-2016-14:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.255.36.86	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
71.6.135.131	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
84.20.63.93	Switzerland	147.237.77.74	law.idf.il	14331: HTTP: Suspicious User-Agent (My Session)	Block	1

08-29-2016-13:04:06 to 08-29-2016-14:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
167.114.17.147	147.237.77.216	Canada	dover.idf.il	Tehila - Perl LWP with fake user agent	14
79.180.17.210	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	4
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
201.238.202.219	147.237.76.39	Chile	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.76.83	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
185.120.126.19	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.116.84.209	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.115	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.132.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.184	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.26.98	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.70.25.105	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.132.18.38	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.33.234	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.47	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.181.48.180	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.150.133.226	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.143.218	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
201.238.202.219	147.237.76.38	Chile	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
46.120.150.14	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.228.202.18	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.116.21.192	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.68.140.207	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.5	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.130.82	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.202	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.217.181	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.81.220.4	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
216.72.34.217	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.80.162	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

08-29-2016-13:04:06 to 08-29-2016-14:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
15.219.201.83	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
89.46.180.223	Palestinian Territory, Occupied	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	10
199.203.179.99	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
40.77.169.102	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
106.38.241.105	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	6
46.19.85.191	Israel	147.237.72.166	aka.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	3
192.169.7.223	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	3
109.253.139.97	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
109.253.201.204	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
176.13.244.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
106.38.241.105	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
176.13.17.4	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.247.187	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
37.247.36.81	Netherlands	147.237.76.34	yohalan.idf.il	drop		drop	1
201.238.202.219	Chile	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
176.13.225.226	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
184.105.139.79	United States	147.237.0.33	idf.il	drop		drop	1
109.253.199.179	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
176.13.229.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
106.38.241.105	China	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
176.13.230.2	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	1
106.38.241.105	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
176.13.7.143	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
79.176.59.36	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1

08-29-2016-13:04:06 to 08-29-2016-14:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.161.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	147
2.53.20.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
176.13.230.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
46.19.85.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
46.19.86.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
176.13.13.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
46.19.86.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
77.139.69.181	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	4
167.114.17.147	Canada	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 167.114.17.147	Block	4
62.219.147.212	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	4
80.246.138.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.33.77	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	3
109.253.222.233	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.6	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
62.219.147.212	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 62.219.147.212	Block	3
2.53.171.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
207.46.13.109	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
80.246.139.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.193.219	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
2.53.149.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.76.35	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.35	Block	2
84.94.43.110	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
46.19.86.122	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
91.233.55.16	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
109.226.49.238	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	1
62.219.147.212	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/163-7238-he/	Block	1
84.109.138.36	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/163-7238-he/patzar.aspxundefined	Block	1
37.142.183.36	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
157.55.39.101	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.76.37	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
101.178.206.92	Australia	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/jetspeed/	Block	1
31.168.11.194	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	1
192.115.177.202	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.115.177.202	Block	1
66.102.9.21	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
84.111.140.16	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.53.57.39	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$questionUpdate$comboQuestion in www.aka.idf.il/main/giyus/faq.aspx	None	1
212.25.79.133	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
77.139.156.11	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
157.55.39.240	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/tizmoret/gallery/	None	1
66.249.76.46	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.46	Block	1
62.0.53.43	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
101.178.206.92	Australia	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/vsapres/web20/core/login.aspx	Block	1
82.19.114.199	United Kingdom	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
31.168.11.194	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/7/	Block	1
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
192.118.10.10	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.118.10.10	Block	1
66.102.9.24	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
87.69.221.189	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

08-29-2016-13:04:06 to 08-29-2016-14:04:06