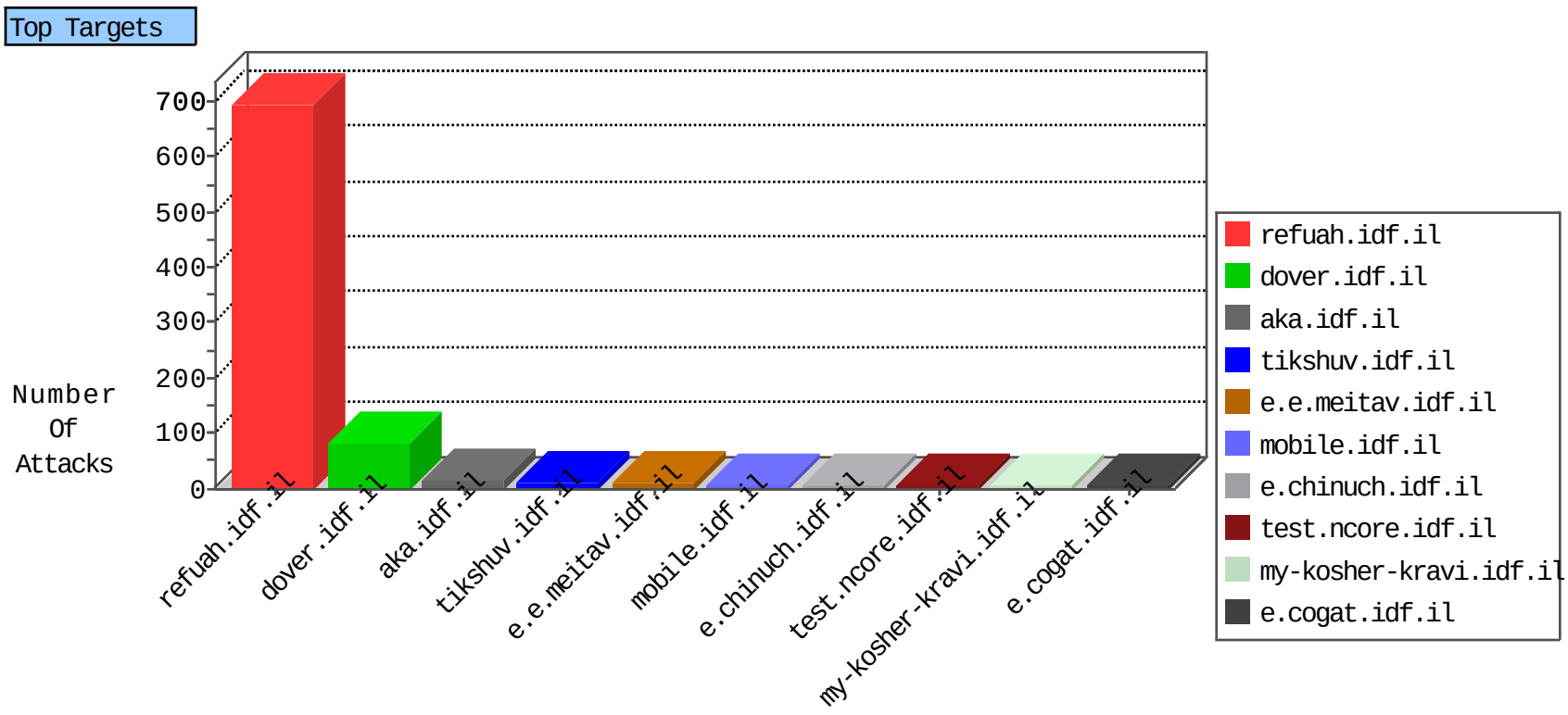
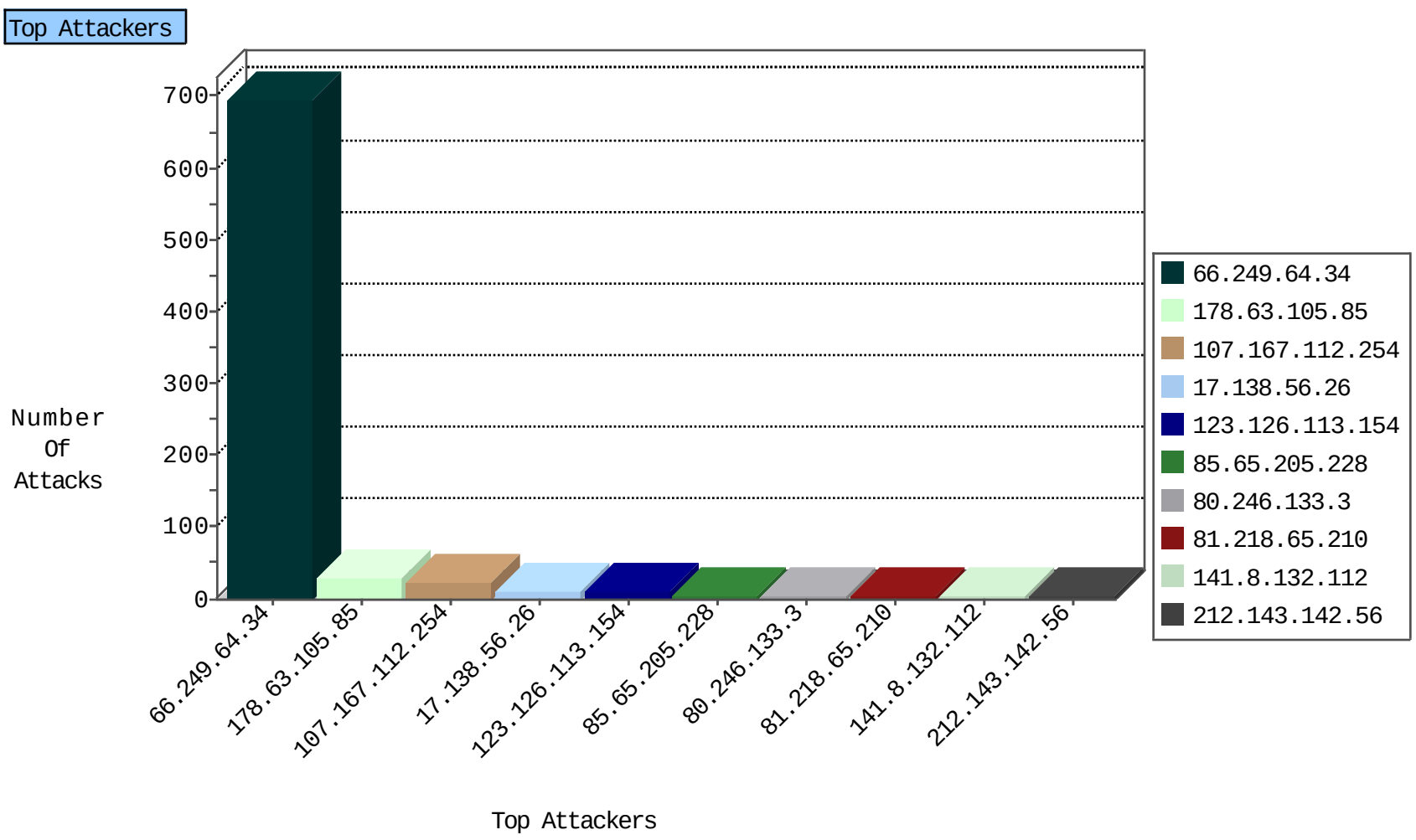
03-07-2016-05:04:01 to 03-07-2016-06:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-07-2016-05:04:01 to 03-07-2016-06:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
185.103.252.5		147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	4
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.116	United States	147.237.77.212	e.dover.idf.il	Block_Ntp_All_Net	drop	1
108.186.168.25	United States	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
185.56.28.67	Netherlands	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.96	United States	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
66.240.219.146	United States	147.237.8.14	e.orchot.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.120	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
108.186.168.25	United States	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.104	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Ntp_All_Net	drop	1
74.82.47.10	United States	147.237.77.205	prisha.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.120	United States	147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.68	United States	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.104	United States	147.237.8.46	e.chinuch.idf.il	Block_Ntp_All_Net	drop	1
184.105.247.216	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.80	United States	147.237.72.217	e.idf.il	Block_Ntp_All_Net	drop	1

03-07-2016-05:04:01 to 03-07-2016-06:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.154	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	7
80.246.133.3	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
46.165.197.142	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
75.127.10.176	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
83.130.126.149	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
104.168.147.242	United States	147.237.77.176	matpash.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1

03-07-2016-05:04:01 to 03-07-2016-06:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.64.34	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	696
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
59.46.193.114	147.237.8.46	China	e.chinuch.idf.il	GPL SCAN nmap TCP	2
213.163.117.221	147.237.76.30	Albania	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.232.98.38	147.237.77.227		e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
218.108.132.58	147.237.77.19	China	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
218.24.171.223	147.237.8.46	China	e.chinuch.idf.il	GPL SCAN nmap TCP	1
213.163.117.221	147.237.0.35	Albania	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
159.122.254.212	147.237.76.148	Netherlands	gqcenter.aka.idf.i	ET SCAN Potential SSH Scan	1
219.84.98.112	147.237.76.31	Taiwan	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
218.108.132.58	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1

03-07-2016-05:04:01 to 03-07-2016-06:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
107.167.112.254	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	22
178.63.105.85	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	9
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
178.63.105.85	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	5
178.63.105.85	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
178.63.105.85	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	3
123.126.113.154	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.253.214.183	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	3
37.46.39.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
209.171.88.184	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
178.63.105.85	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	2
85.65.205.228	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
184.105.139.104	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
123.125.71.27	China	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.8	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.131	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
218.22.211.69	China	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
66.130.253.221	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.247.247	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
123.126.113.80	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
74.82.47.20	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
178.63.105.85	Germany	147.237.77.243	mobile.idf.il	drop	SAM rule	drop	1
141.212.122.134	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
66.130.253.221	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
195.62.53.168	Russian Federation	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
178.63.105.85	Germany	147.237.76.39	mobile.meitav.idf.il	drop	SAM rule	drop	1
74.82.47.24	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.84	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.99	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.135	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
66.176.140.214	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
197.164.86.134	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.24	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.90	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.99	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
121.54.44.92	Philippines	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.7	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
198.20.70.114	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.130	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
85.25.43.94	Germany	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.119	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

03-07-2016-05:04:01 to 03-07-2016-06:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
17.138.56.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.56.26	Block	12
85.65.205.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
141.212.122.129	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to /x	Block	1
66.249.64.235	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
37.26.147.162	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
196.221.237.247	Egypt	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
79.180.201.41	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
66.249.64.131	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
157.55.39.183	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
66.249.66.44	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
46.19.85.232	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
208.115.113.89	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/templatecontrols/news/sip_storage/files/6/1446.pdf/	Block	1
66.249.64.137	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
188.120.148.64	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
66.249.66.188	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
49.177.22.136	Australia	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
216.218.206.66	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
85.65.205.228	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	1
66.249.64.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
188.120.148.64	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/xmlrpc.php	Block	1
66.249.69.77	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/24012011yezu.aspx	Block	1
66.90.183.203	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
106.184.7.86	Japan	147.237.72.166	aka.idf.il	Unknown Parameter catid in www.aka.idf.il/patzar/home/default.asp	None	1
66.249.64.233	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/key/aswd56425csa	Block	1
196.221.237.247	Egypt	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
74.103.152.197	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.90.183.203	United States	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1

03-07-2016-05:04:01 to 03-07-2016-06:04:01