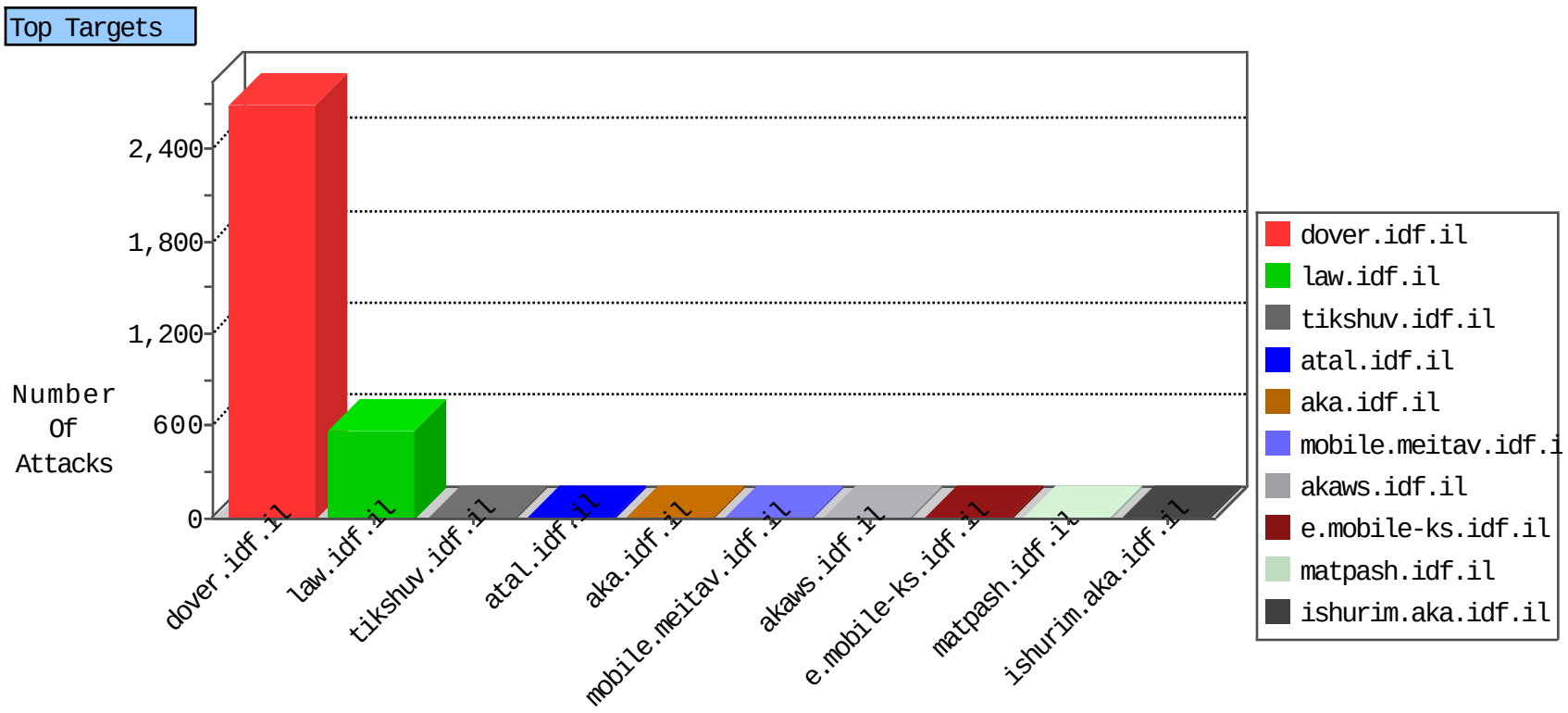
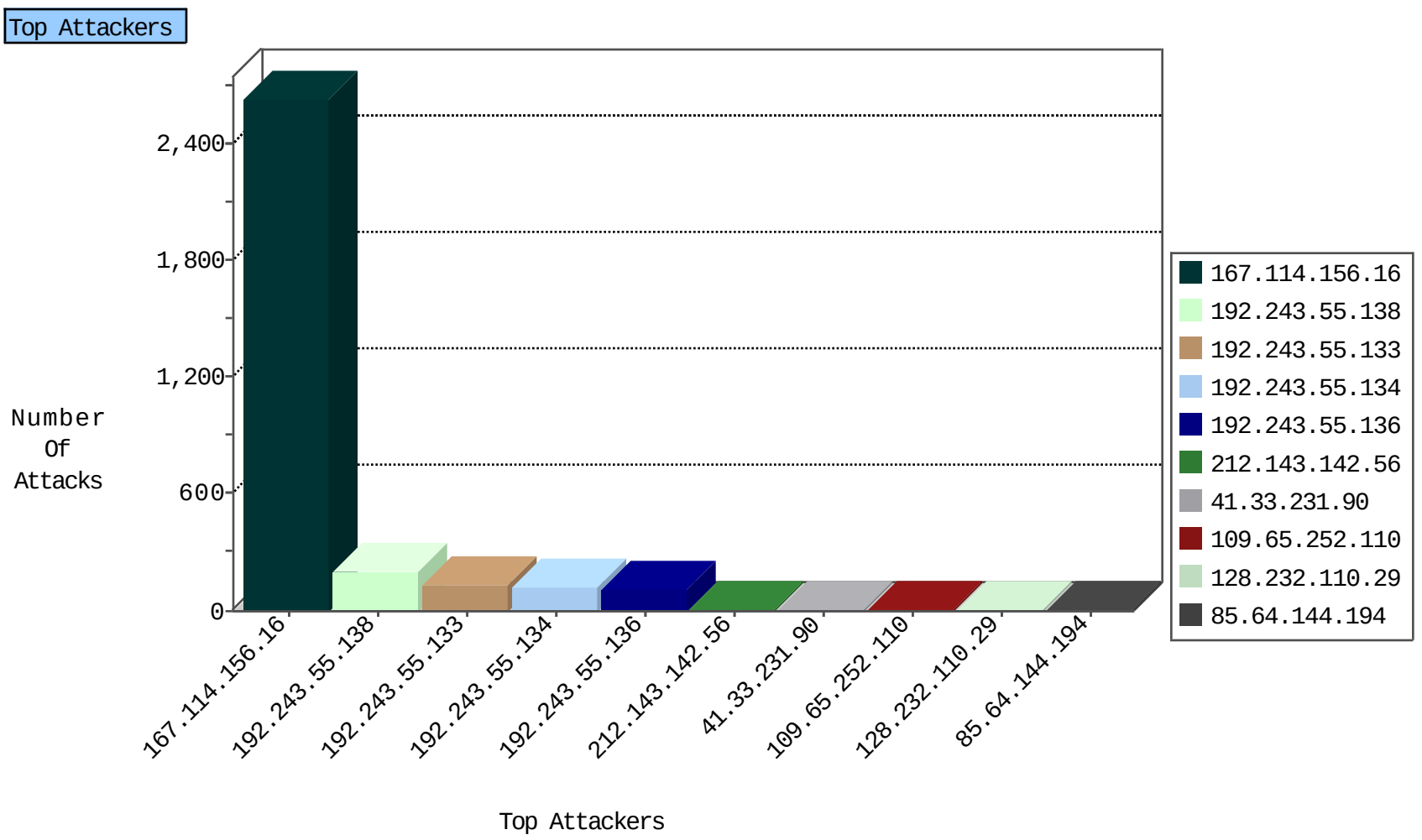
04-13-2016-05:04:09 to 04-13-2016-06:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-13-2016-05:04:09 to 04-13-2016-06:04:09

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	Block_Ip_Web_In	drop	2623
72.36.244.208	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
184.164.195.68	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
184.105.139.84	United States	147.237.77.61	e.cogat.idf.il	Block_Ntp_All_Net	drop	1
82.136.39.51	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
213.52.178.162	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
184.164.195.18	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
179.43.144.31	Switzerland	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
72.36.244.209	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
202.88.1.3	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
184.105.139.96	United States	147.237.77.243	mobile.idf.il	Block_Ntp_All_Net	drop	1
101.0.101.183	Australia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
213.52.178.165	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
184.164.195.22	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
179.43.144.31	Switzerland	147.237.8.24	e.lifestyle.idf.il	Block_Ntp_All_Net	drop	1
72.36.244.210	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
202.88.1.4	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
184.105.139.100	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
103.29.5.8	Indonesia	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
184.164.195.29	United States	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
179.43.144.31	Switzerland	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
74.82.47.46	United States	147.237.0.16	my-kosher-kravi.idf.il	Block_Udp_All_Nets	drop	1
202.88.1.10	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
184.105.139.100	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	1

04-13-2016-05:04:09 to 04-13-2016-06:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.252.110	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
92.176.142.53	France	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-13-2016-05:04:09 to 04-13-2016-06:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.65.37	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
98.119.105.221	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 2048	1
98.119.105.221	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -f -sS	1
40.84.159.128	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
190.29.23.197	147.237.8.28	Colombia	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
128.127.0.45	147.237.76.39	Italy	mobile.meitav.idf.i	ET SCAN NMAP -sS window 2048	1
113.240.250.154	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
98.119.105.221	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.79.104	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
40.84.159.128	147.237.8.45	United States	e.eitan.idf.il	ET SCAN NMAP -sS window 3072	1
163.172.140.23	147.237.76.34	United Kingdom	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
128.127.0.45	147.237.76.39	Italy	mobile.meitav.idf.i	ET SCAN NMAP -f -sS	1

04-13-2016-05:04:09 to 04-13-2016-06:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	45
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	42
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	40
192.243.55.138	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	37
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	33
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	31
192.243.55.138	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	31
192.243.55.133	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	28
192.243.55.134	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	27
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	23
192.243.55.134	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	22
192.243.55.138	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	21
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
192.243.55.136	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
192.243.55.136	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	18
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	17
192.243.55.136	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	18
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	17
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	14
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
192.243.55.133	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	10
185.106.92.47	Russian Federation	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	5
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	4
37.205.0.49	Turkey	147.237.77.233	atal.idf.il	drop	SAM rule	drop	4
89.204.137.57	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.66.47	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.51.230	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.64.144.194	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
128.232.110.29	United Kingdom	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
89.204.137.57	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
207.46.13.134	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.177.98.223	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
192.243.55.138	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
85.64.144.194	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
128.232.110.29	United Kingdom	147.237.0.35	akaws.idf.il	drop		drop	2
128.232.110.29	United Kingdom	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
141.212.122.199	United States	147.237.0.35	akaws.idf.il	drop		drop	1
159.226.95.66	China	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
207.46.13.134	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
74.82.47.51	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.39.222.159	Netherlands	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
178.162.205.5	Germany	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.78	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.203	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

04-13-2016-05:04:09 to 04-13-2016-06:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
157.55.39.104	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.66.186	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.186	Block	1
91.121.141.219	France	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/163-7183-en/patzaraspx	Block	1
5.196.21.114	France	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/test/wp-admin/	Block	1
184.168.200.74	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/wp-admin/	Block	1
68.180.230.184	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	1
124.188.99.81	Australia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
45.45.135.2	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
192.243.55.138	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/templates/templatecontrols/news/לכתבה המלאה	Block	1
75.49.253.248	United States	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
131.253.25.250	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.65.37	Israel	147.237.77.74	law.idf.il	Parameter Type Violation SearchText in www.law.idf.il/163-6639-he/patzar.aspx	Block	1
212.97.132.209	Denmark	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/wordpress/wp-admin/	Block	1
75.49.253.248	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
5.39.222.159	Netherlands	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
157.55.39.42	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/sachar/klali.aspx	None	1
66.249.66.128	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	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
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-8517-he/atal.aspx	Block	1
5.39.222.159	Netherlands	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1

04-13-2016-05:04:09 to 04-13-2016-06:04:09