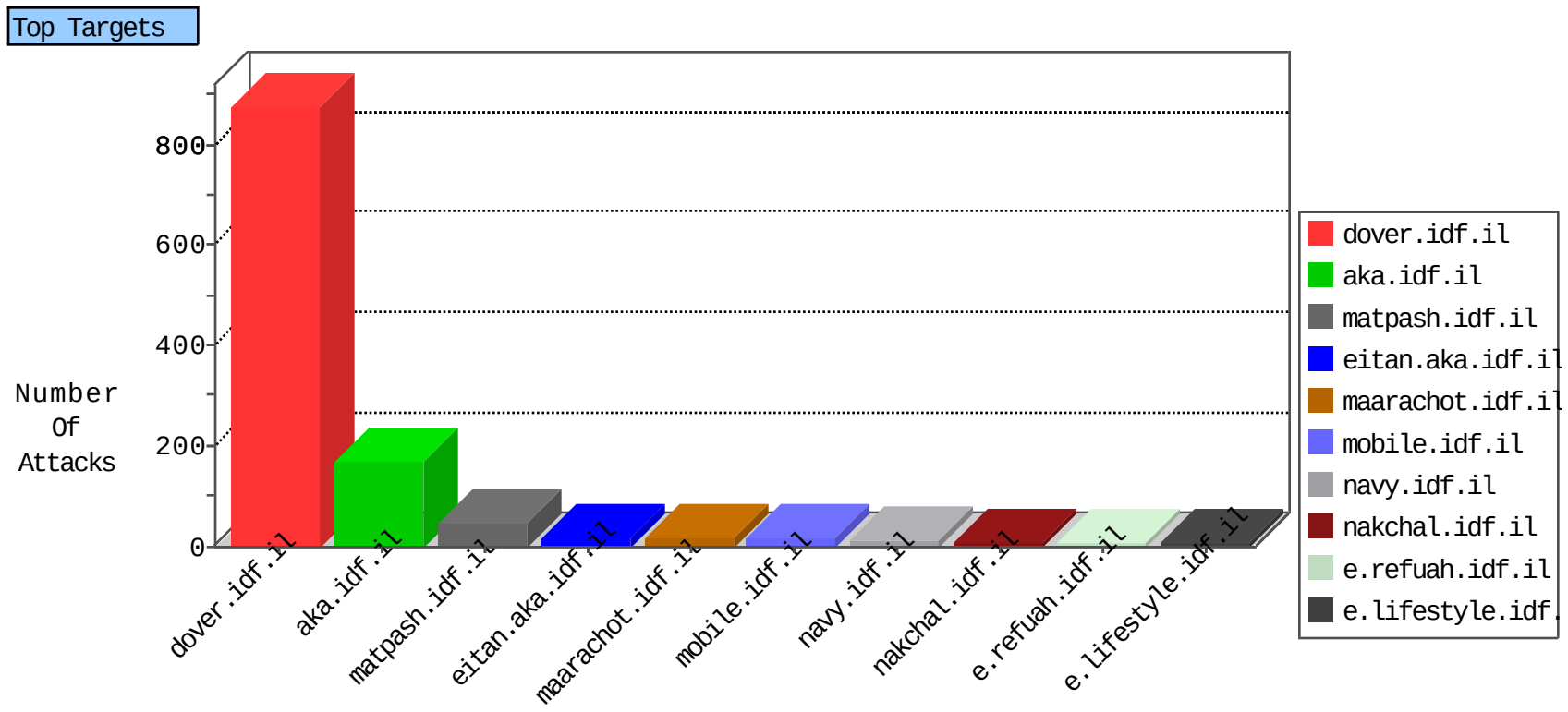
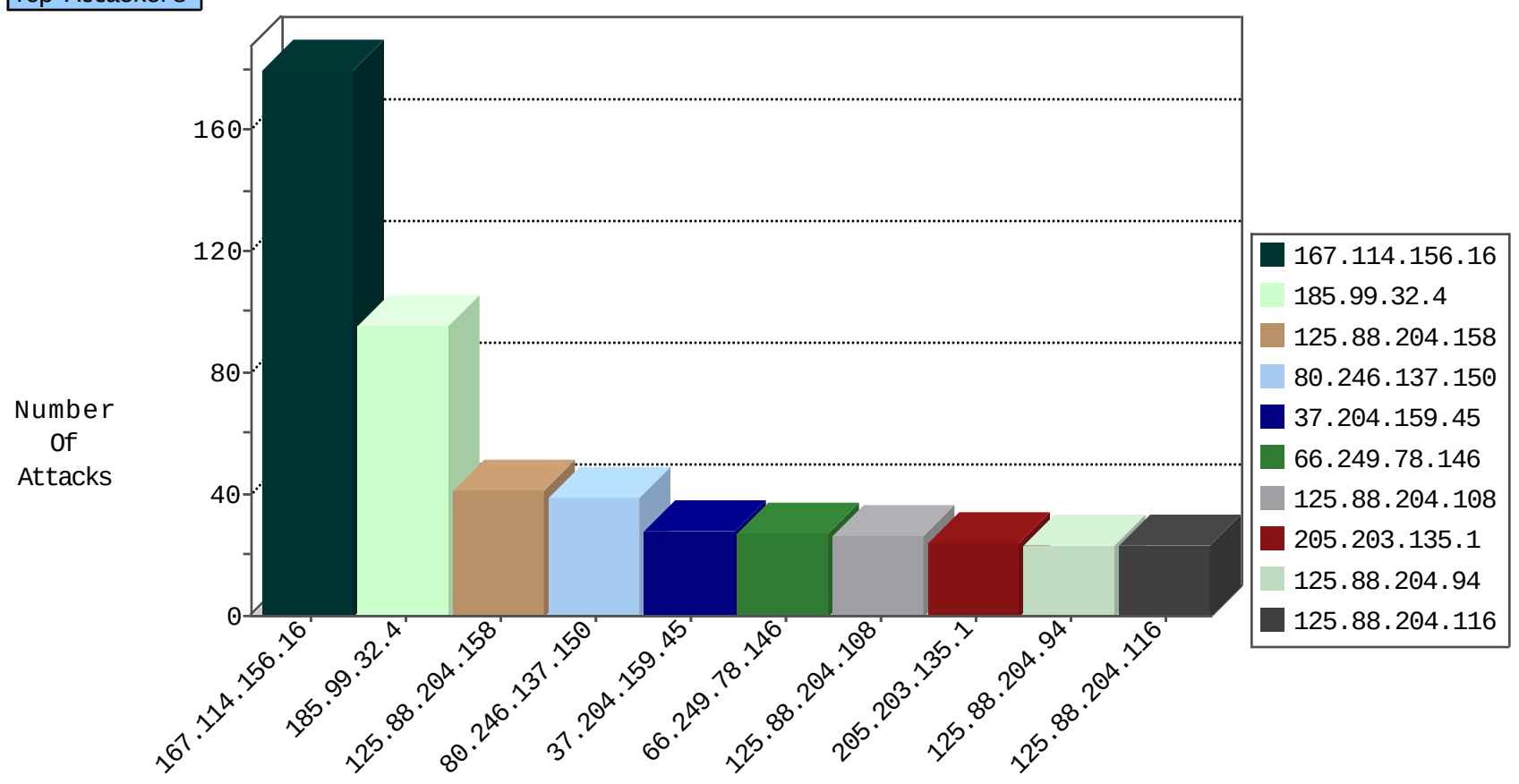
04-27-2016-00:04:08 to 04-27-2016-01:04:08

IDF Under Attack
Daily Report

Top Targets



Top Attackers



04-27-2016-00:04:08 to 04-27-2016-01:04:08

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	HTTP-POST-Segmented-DoS	dest-reset	5516
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	4967
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	4
79.178.40.154	Israel	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	2
185.130.5.48	Lithuania	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.48	Lithuania	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
89.241.254.16	United Kingdom	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	1
185.130.5.48	Lithuania	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.48	Lithuania	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.48	Lithuania	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.116	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.48	Lithuania	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.48	Lithuania	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.116	Netherlands	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.48	Lithuania	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.48	Lithuania	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.116	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1

04-27-2016-00:04:08 to 04-27-2016-01:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-27-2016-00:04:08 to 04-27-2016-01:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.64.233	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	2
115.182.17.13	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.158	147.237.76.86	Ukraine	navy.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.158	147.237.76.86	Ukraine	navy.idf.il	ET SCAN NMAP -f -sS	1
40.76.60.52	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 2048	1
198.23.113.23	147.237.76.86	United States	navy.idf.il	ET SCAN Potential SSH Scan	1
24.24.216.44	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
198.23.113.23	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	1
198.23.113.23	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
187.160.94.228	147.237.77.234	Mexico	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
95.154.250.21	147.237.76.39	United Kingdom	mobile.meitav.idf.i	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.76.86	Ukraine	navy.idf.il	ET SCAN NMAP -sS window 2048	1
80.82.78.38	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
40.76.60.52	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 4096	1
40.76.60.52	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -f -sS	1
198.23.113.23	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential SSH Scan	1
198.23.113.23	147.237.76.30	United States	himush.idf.il	ET SCAN Potential SSH Scan	1

04-27-2016-00:04:08 to 04-27-2016-01:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.99.32.4	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	96
125.88.204.158	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
125.88.204.108	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
125.88.204.116	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
125.88.204.94	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
2.53.23.237	Israel	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
5.90.234.82	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
125.88.204.141	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
87.70.79.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
125.88.204.178	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
37.204.159.45	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	14
37.204.159.45	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
203.133.169.231	Korea, Republic of	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
125.88.204.177	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.92	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
207.46.13.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
40.77.167.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
82.102.205.127	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
80.246.137.150	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
109.67.237.20	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
198.58.102.95	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
78.189.162.108	Turkey	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
188.161.58.244	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
40.77.167.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.249.93.115	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
207.46.13.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
157.55.2.168	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
80.246.137.150	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
80.246.137.150	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
80.246.137.150	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
104.155.92.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.26.148.230	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.26.149.189	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
66.249.93.111	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.0.118.17	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
167.136.142.166	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
105.154.232.153	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

04-27-2016-00:04:08 to 04-27-2016-01:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.228.0.53	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation CurrentPassword in mobile.idf.il/sachar/changepassword	Block	11
78.164.254.231	Turkey	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 78.164.254.231	Block	6
105.154.232.153	Morocco	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/homepage/www.youtube.com/v/3g51ei5nuhg	Block	6
78.164.254.231	Turkey	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	5
78.164.254.231	Turkey	147.237.77.170	maarachot.idf.il	Multiple Admin Blocking from 78.164.254.231	Block	4
46.19.85.51	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.146.134	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en	Block	2
86.28.81.125	United Kingdom	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 86.28.81.125	Block	2
207.46.13.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
82.166.247.200	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/news/mobile	Block	1
66.249.78.130	Israel	147.237.76.86	navy.idf.il	Parameter Type Violation DocID in www.navy.idf.il/navy/general.aspx	Block	1
157.55.12.80	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.5	Israel	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/apple-app-site-association	Block	1
207.119.114.12	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.154	Israel	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
212.106.72.215	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
5.39.222.159	Netherlands	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
86.28.81.125	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/homepage/mobile	Block	1
66.249.78.161	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
51.255.65.63	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/html/toolfs.asp	Block	1
194.28.112.50	Netherlands	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
212.143.40.198	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
31.154.168.181	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1361-he/dover.aspx	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
203.133.169.231	Korea, Republic of	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
78.164.254.231	Turkey	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
66.249.78.104	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/8/113338.pdf	Block	1
37.26.146.134	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
141.212.122.161	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
78.164.254.231	Turkey	147.237.77.170	maarachot.idf.il	Admin Blocking	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2308.jpg	Block	1

04-27-2016-00:04:08 to 04-27-2016-01:04:08