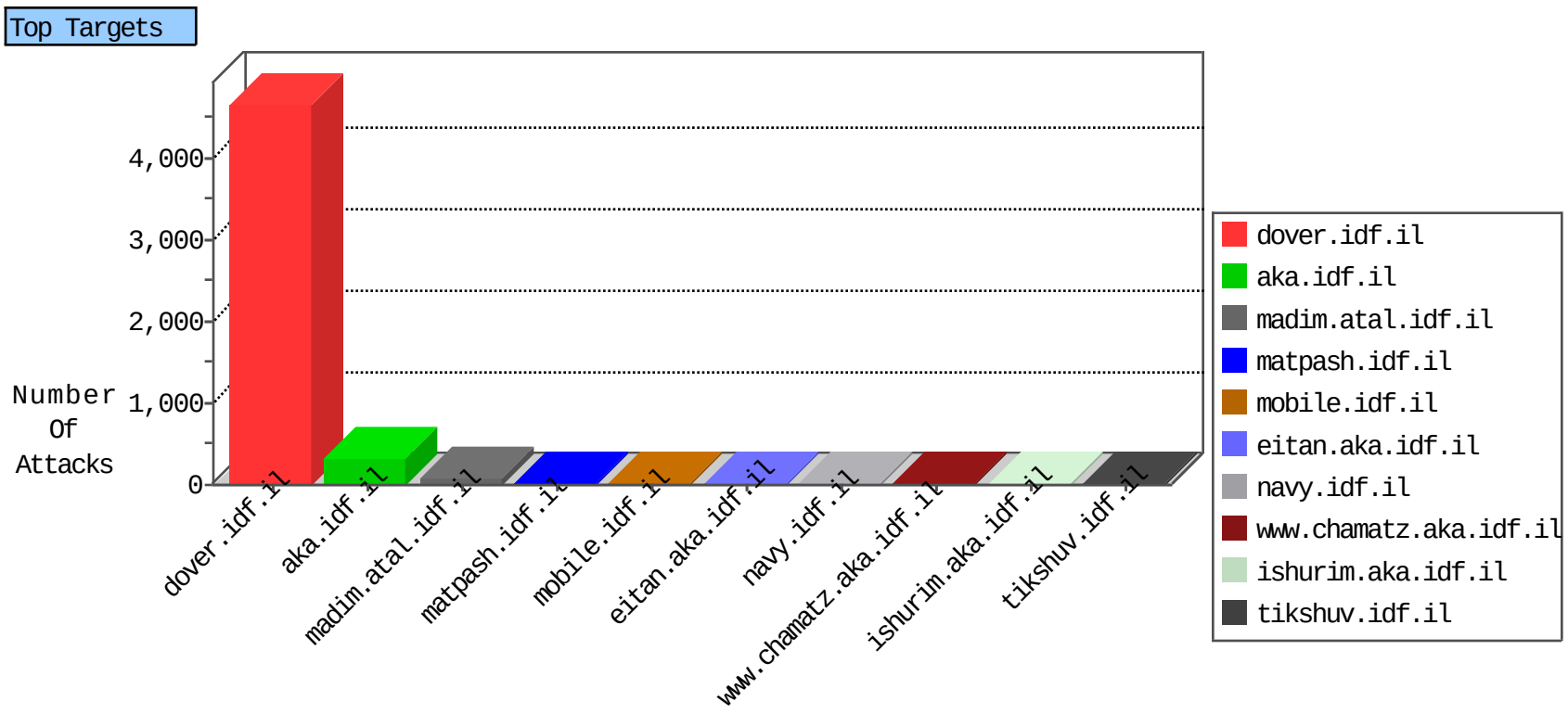
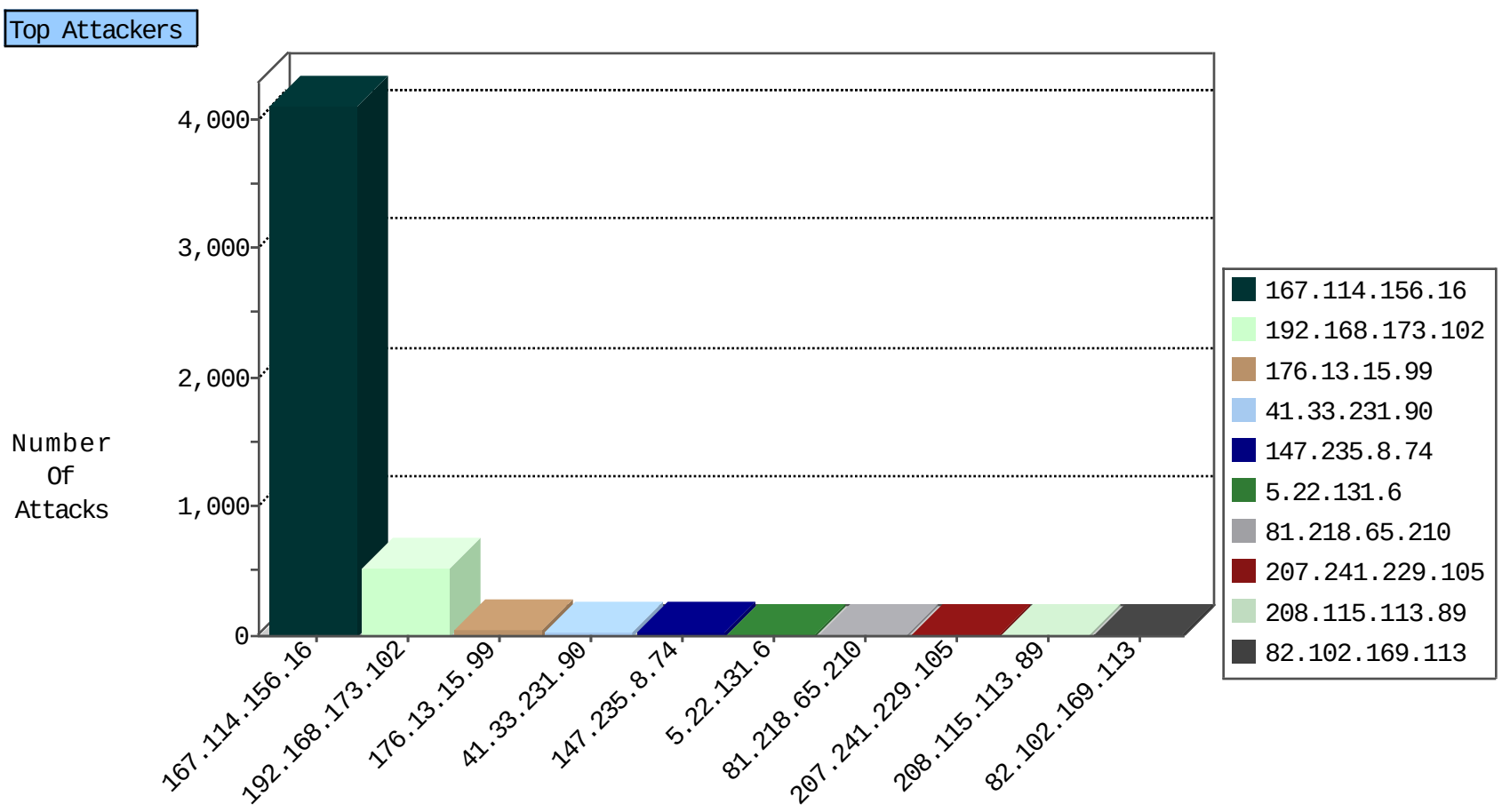
04-10-2016-07:04:09 to 04-10-2016-08:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-10-2016-07:04:09 to 04-10-2016-08:04:09

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	4110
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	15
82.145.209.47	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4
209.126.127.17	United States	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	2
109.64.11.232	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
209.126.127.17	United States	147.237.72.217	e.idf.il	Block_Udp_All_Nets	drop	2
82.145.220.69	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	2
184.105.139.88	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1
192.3.220.210	United States	147.237.8.28	e.mobile-ks.idf.il	Block_Udp_All_Nets	drop	1
93.172.136.160	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
184.105.139.116	United States	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.124	United States	147.237.0.34	tikshuv.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1

04-10-2016-07:04:09 to 04-10-2016-08:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.30.219.2	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	5
213.251.184.38	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.211.2	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
213.251.184.38	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	1
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
120.156.4.171	Australia	147.237.77.170	maarachot.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
157.55.39.201	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
207.46.13.45	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-10-2016-07:04:09 to 04-10-2016-08:04:09

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
88.204.187.90	147.237.77.216	Kazakstan	dover.idf.il	ET SCAN NMAP -f -sS	1
46.151.52.139	147.237.77.178	Ukraine	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
222.114.11.202	147.237.0.35	Korea, Republic of	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
218.108.132.58	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 1024	1
152.238.214.216	147.237.77.216	Brazil	dover.idf.il	portscan: TCP Distributed Portscan	1
88.204.187.90	147.237.77.216	Kazakstan	dover.idf.il	ET SCAN NMAP -sS window 2048	1
61.136.166.210	147.237.72.166	China	aka.idf.il	portscan: TCP Distributed Portscan	1
218.108.132.58	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
213.8.54.140	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.77.91.113	147.237.0.16	Turkey	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
109.253.210.103	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

04-10-2016-07:04:09 to 04-10-2016-08:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	344
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	181
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
5.22.131.6	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
207.241.229.105	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	13
208.115.113.89	United States	147.237.77.216	dover.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	10
46.19.85.181	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
82.102.169.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
147.235.8.74	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
147.235.8.74	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
147.235.8.74	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
46.19.86.221	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	8
109.66.68.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.130.2	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
80.179.9.115	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.154	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
80.246.137.149	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.179.119.22	Israel	147.237.76.86	navy.idf.il	drop	SAM rule	drop	6
176.13.1.130	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.124.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
106.38.241.149	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
37.26.149.188	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.183	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
46.19.85.112	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.86.99	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.248.252	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
69.30.219.2	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.85.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.184.30	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.178.157.110	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
207.232.37.85	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.108	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
109.67.158.123	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.188	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
2.55.1.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.158.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
91.135.102.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.50.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
222.89.166.26	China	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
2.53.62.128	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.182.104.17	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.27.105.115	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.63.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.82.24.37	Senegal	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	2
185.27.105.165	Israel	147.237.77.216	dover.idf.il	drop		drop	2
37.26.148.196	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2

04-10-2016-07:04:09 to 04-10-2016-08:04:09

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
46.19.85.181	Israel	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	2
185.27.105.165	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2

04-10-2016-07:04:09 to 04-10-2016-08:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.15.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
109.253.134.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
157.55.39.205	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
176.13.22.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
149.78.69.250	United States	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
186.220.160.173	Brazil	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.253.142.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	2
169.229.3.90	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/rec.dat	Block	1
77.237.138.202	Czech Republic	147.237.77.234	halag.idf.il	Unauthorized URL Access to /	Block	1
46.19.86.179	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.102.7.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
207.46.13.21	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.21	Block	1
40.77.167.6	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
80.246.137.149	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
54.153.32.246	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	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
66.249.65.12	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
41.107.254.195	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.107.254.195	Block	1
54.153.33.152	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
192.118.10.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/1.he/back.png	Block	1
66.249.65.217	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
41.107.254.195	Algeria	147.237.77.216	dover.idf.il	Parameter Type Violation ID in www.idf.il/1294-ar/dover.aspx	Block	1
184.105.139.68	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/images/shared/newsitemback.gif	Block	1
54.153.33.152	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
200.187.64.91	Brazil	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 200.187.64.91	Block	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-16789-he/dover.aspx	Block	1
41.107.254.195	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1361-ar/dover.aspx^	Block	1
185.27.105.165	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/favicon.ico	Block	1
89.234.68.69	Ireland	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.102.7.226	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
200.187.64.91	Brazil	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1

04-10-2016-07:04:09 to 04-10-2016-08:04:09