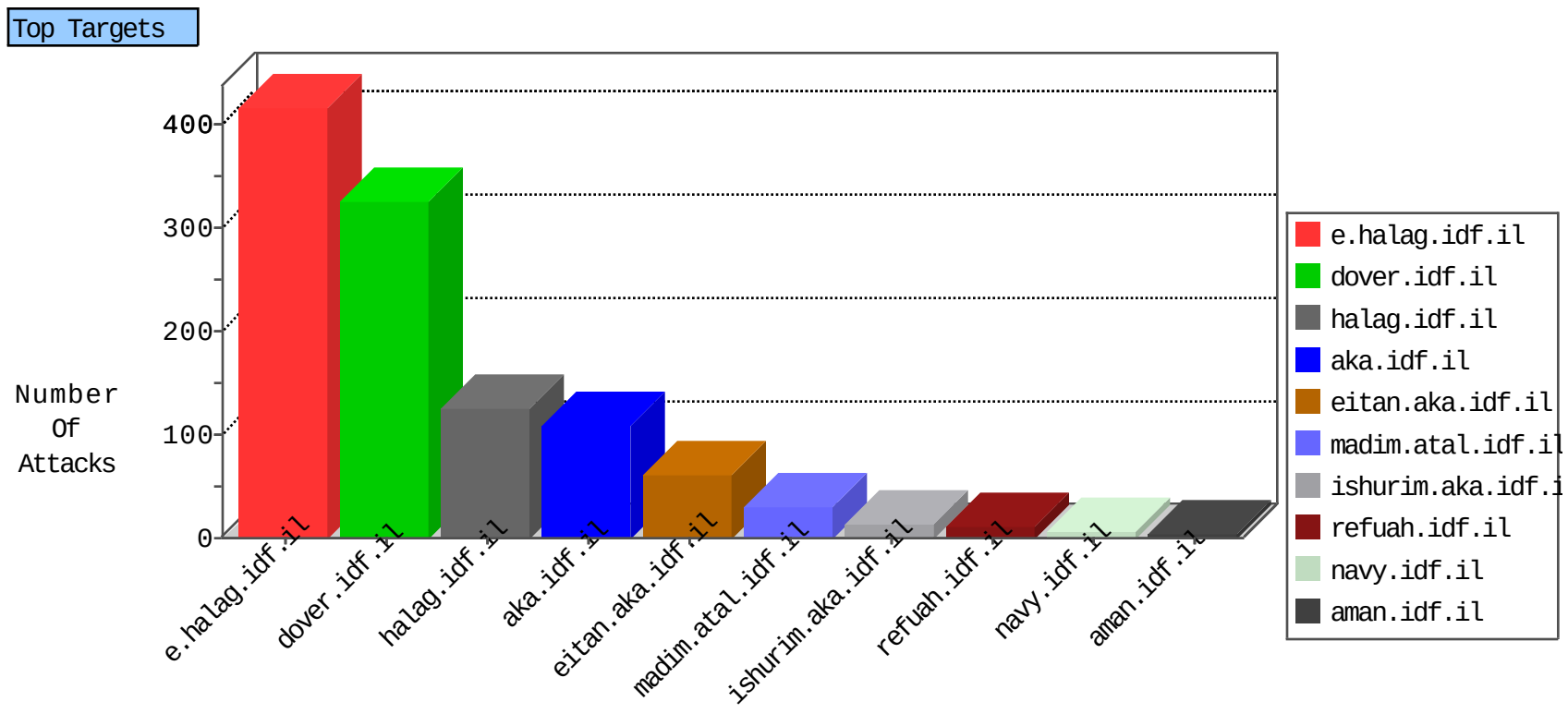
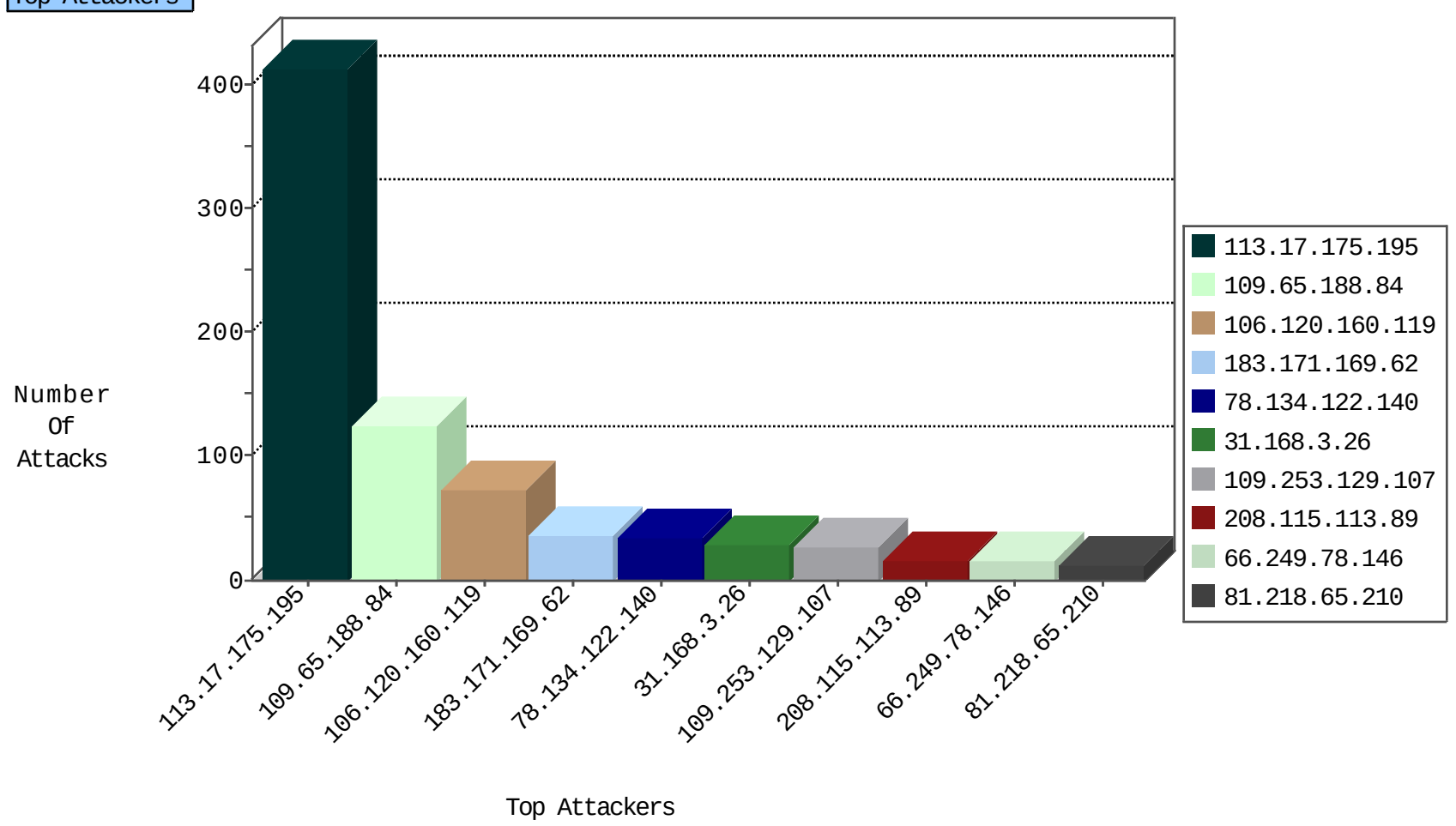
04-25-2016-07:04:05 to 04-25-2016-08:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-25-2016-07:04:05 to 04-25-2016-08:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
113.17.175.195	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	414
167.114.156.16	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	15
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	9
81.218.65.210	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
212.179.64.162	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
192.249.66.247	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
5.196.72.168	France	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
120.132.50.135	China	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	drop	1
198.20.69.74	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	1

04-25-2016-07:04:05 to 04-25-2016-08:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-25-2016-07:04:05 to 04-25-2016-08:04:05

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
66.102.8.222	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
110.159.147.221	147.237.77.216	Malaysia	dover.idf.il	Xenu Link Sleuth User Agent	2
61.6.250.16	147.237.76.30	Brunei Darussalam	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
23.96.109.87	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
223.4.174.30	147.237.76.42	China	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
124.105.93.102	147.237.76.30	Philippines	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
106.184.2.29	147.237.8.46	Japan	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.155	147.237.76.39	Ukraine	mobile.meitav.idf.i	ET SCAN NMAP -sS window 3072	1
23.96.109.87	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 4096	1
223.4.174.30	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
223.4.174.30	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
179.228.8.178	147.237.0.35	Brazil	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.155	147.237.76.39	Ukraine	mobile.meitav.idf.i	ET SCAN NMAP -sS window 4096	1
87.229.116.42	147.237.77.216	Hungary	dover.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1

04-25-2016-07:04:05 to 04-25-2016-08:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.65.188.84	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	124
106.120.160.119	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	73
183.171.169.62	Malaysia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
78.134.122.140	Italy	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
31.168.3.26	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
87.69.255.212	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
157.55.39.38	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
82.102.169.113	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
149.202.48.207	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
207.46.13.34	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
157.55.39.224	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
217.115.10.132	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.93.182	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
94.159.180.147	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
106.120.165.96	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
67.44.208.172	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.64.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
105.93.165.224	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.218.217.197	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
106.120.164.250	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
87.70.77.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.108.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.55.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.251.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.70.180	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.156.128	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.179.9.115	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
65.55.210.133	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
2.53.164.105	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.7.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.179.13.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
84.110.208.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.245	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.70.23.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.155.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-25-2016-07:04:05 to 04-25-2016-08:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.129.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	5
185.3.144.127	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	2
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-17082-en/	Block	1
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
66.249.64.239	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	1
213.57.185.135	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl67 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
109.72.215.18	United Kingdom	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/index.php	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1398-en/dover.aspx	Block	1
31.154.41.17	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
149.202.48.207	France	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/1050-he/patzar.aspxבדק	Block	1
85.64.213.204	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/he-1133/dover.aspx	Block	1
66.249.66.47	Israel	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on tikshuv.idf.il/main/giyus/general.aspx	Block	1
216.51.232.61	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 216.51.232.61	Block	1
109.72.215.18	United Kingdom	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/index.php	Block	1
74.82.47.2	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
46.117.19.199	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 46.117.19.199	Block	1
149.202.48.207	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1153-230	Block	1
106.186.113.132	Japan	147.237.76.42	refuah.idf.il	Multiple Untraceable SSL Sessions from 106.186.113.132 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/eitan/listpage/	Block	1
80.179.9.7	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.181	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
106.186.113.132	Japan	147.237.76.42	refuah.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.78.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/listpage/	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/giyus/general.aspx	Block	1
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
207.46.13.108	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/sitemap/sitemap.aspx	Block	1
109.65.188.84	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.79.130	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1

04-25-2016-07:04:05 to 04-25-2016-08:04:05