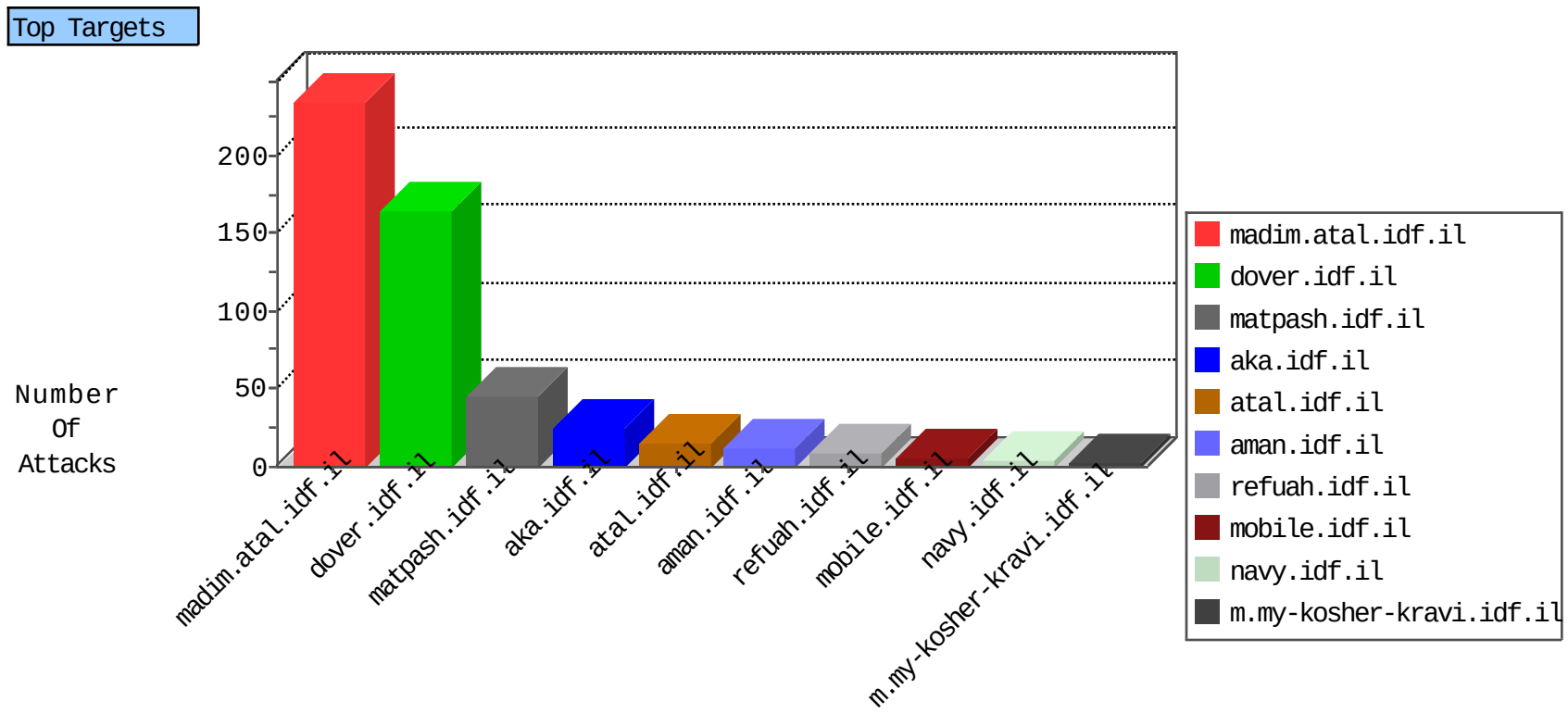
08-22-2016-19:04:03 to 08-22-2016-20:04:03

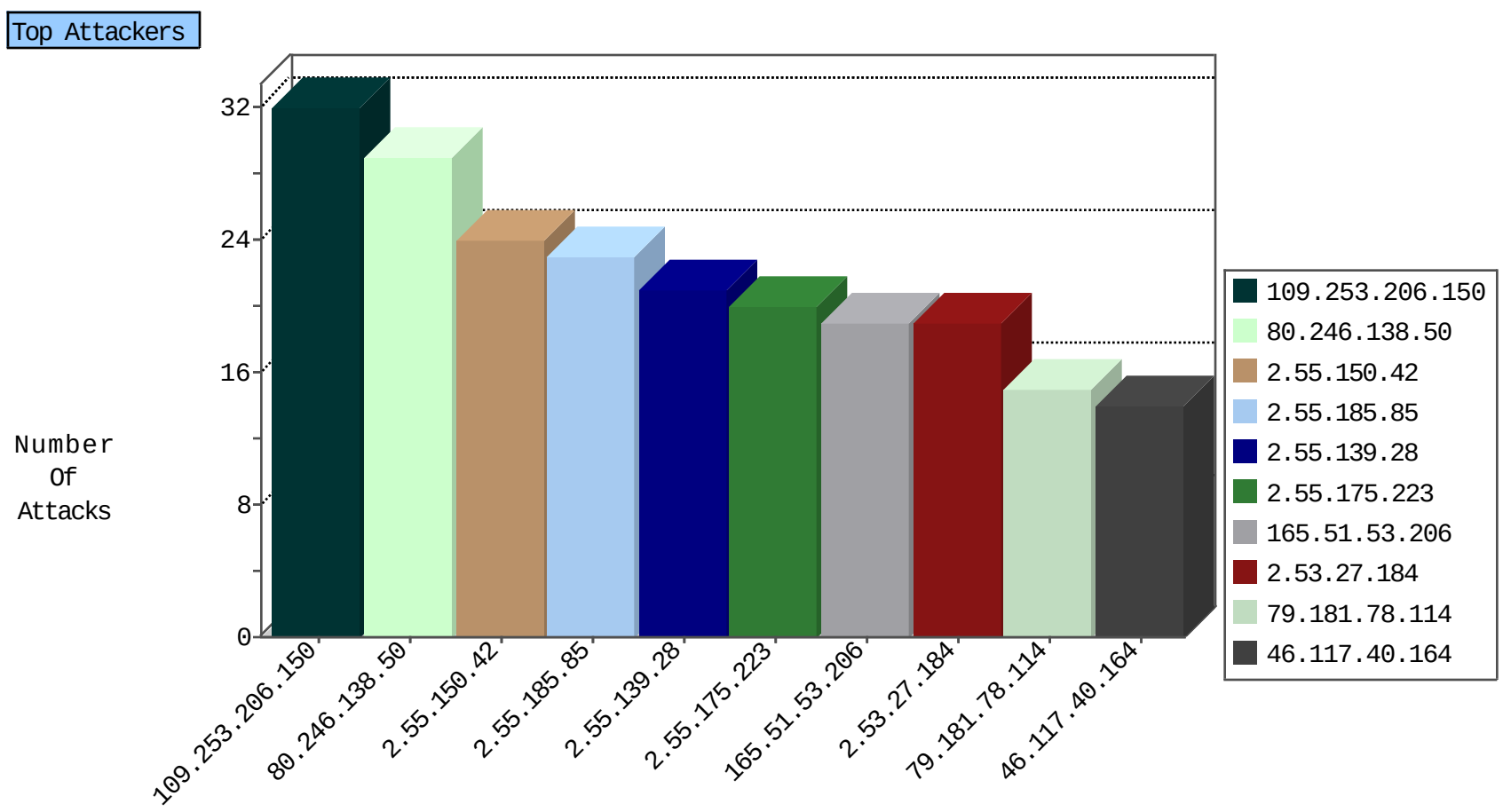
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

08-22-2016-19:04:03 to 08-22-2016-20:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.80.78.2	Israel	147.237.72.166	aka.idf.il	Black List	drop	4
79.183.0.119	Israel	147.237.76.42	refuah.idf.il	Black List	drop	1

08-22-2016-19:04:03 to 08-22-2016-20:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
71.6.165.200	United States	147.237.8.24	e.lifestyle.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
89.248.167.131	Netherlands	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
151.80.31.104	France	147.237.76.200	eitan.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

08-22-2016-19:04:03 to 08-22-2016-20:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
79.181.78.114	147.237.77.233	Israel	atal.idf.il	ET SCAN NMAP -sA (2)	13
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	4
79.181.78.114	147.237.76.42	Israel	refuah.idf.il	ET SCAN NMAP -sA (2)	2
58.218.204.245	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
46.172.71.251	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.225.138	147.237.77.176	Ukraine	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
5.39.222.253	147.237.72.156	Netherlands	aman.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.72.14	United Kingdom	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
92.147.39.133	147.237.0.17	France	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
84.109.38.224	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	1
58.218.204.245	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
58.218.204.245	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
5.42.204.21	147.237.77.216	Iraq	dover.idf.il	ET SCAN NMAP -sA (2)	1
193.34.160.65	147.237.0.16	Russian Federation	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.66.234	147.237.77.179	United Kingdom	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
92.147.39.133	147.237.0.17	France	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
92.147.39.133	147.237.0.17	France	m.my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1

08-22-2016-19:04:03 to 08-22-2016-20:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
197.6.27.136	Tunisia	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	14
109.253.212.214	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
165.51.53.206	Tunisia	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.117	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
165.51.53.206	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.53.55.212	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
188.161.44.8	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.253.144.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
93.131.3.74	Germany	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	7
78.41.149.241	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
188.161.44.8	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	7
5.34.166.144	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
109.253.197.64	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
108.29.98.221	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
100.92.134.25		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.53.176.82	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
213.8.204.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
199.58.86.211	United States	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	4
5.34.166.144	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
109.253.144.18	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
85.64.222.133	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
87.69.206.81	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
87.70.241.25	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.53.145.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.53.169.152	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.253.146.239	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
199.58.86.211	United States	147.237.77.233	atal.idf.il	drop	SAM rule	drop	2
31.223.170.208	Netherlands	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
85.130.174.100	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
80.179.225.42	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
199.58.86.211	United States	147.237.77.234	halag.idf.il	drop	SAM rule	drop	2
41.227.236.196	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
46.121.44.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
2.55.55.24	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
84.229.66.50	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
46.19.85.29	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
176.13.227.166	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
2.53.59.168	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
77.126.0.183	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.130.221	Israel	147.237.0.19	madim.atal.idf.il	drop	First packet isn't SYN	drop	1
176.13.234.11	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.213.225	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
2.53.32.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.136.54	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
85.130.174.100	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	1
216.243.31.2	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
46.19.85.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
185.120.126.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

08-22-2016-19:04:03 to 08-22-2016-20:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.206.150	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	30
80.246.138.50	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	29
2.55.150.42	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	24
2.55.185.85	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	23
2.55.139.28	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
2.55.175.223	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	20
2.53.27.184	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	19
46.117.40.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
37.26.149.218	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
46.19.85.121	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
2.53.177.115	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
2.53.151.33	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.53.133.233	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
2.55.146.250	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
2.55.177.30	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.53.144.245	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
109.253.206.150	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
37.26.148.207	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
89.237.71.54	France	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.53.172.61	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
72.239.171.246	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	2
131.253.25.148	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.53.182.85	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.53.183.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
5.42.204.21	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	2
2.53.180.10	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.176.92.187	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
46.19.86.27	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.78.195.38	Netherlands	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
31.13.100.112	Ireland	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/3016.jpg›	Block	1
89.139.47.9	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$txtPassword in www.aka.idf.il/main/giyus/faq.aspx	None	1
2.53.165.170	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
66.249.93.111	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/uukzk/english/	Block	1
46.19.85.189	Israel	147.237.76.86	navy.idf.il	Abnormally Long Request method	Block	1
79.178.13.52	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
2.53.180.93	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
46.19.86.166	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.53.147.193	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
212.90.60.99	Ukraine	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
46.19.85.189	Israel	147.237.76.86	navy.idf.il	Multiple Malformed URL from 46.19.85.189	Block	1
5.22.131.98	Israel	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
109.67.21.7	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	1
2.55.172.246	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.53.173.62	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.124.45.91	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
46.19.85.189	Israel	147.237.76.86	navy.idf.il	Multiple Unknown HTTP Request Method from 46.19.85.189	Block	1
5.22.131.98	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
157.55.39.38	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.108.82.35	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	1
66.249.79.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1

08-22-2016-19:04:03 to 08-22-2016-20:04:03