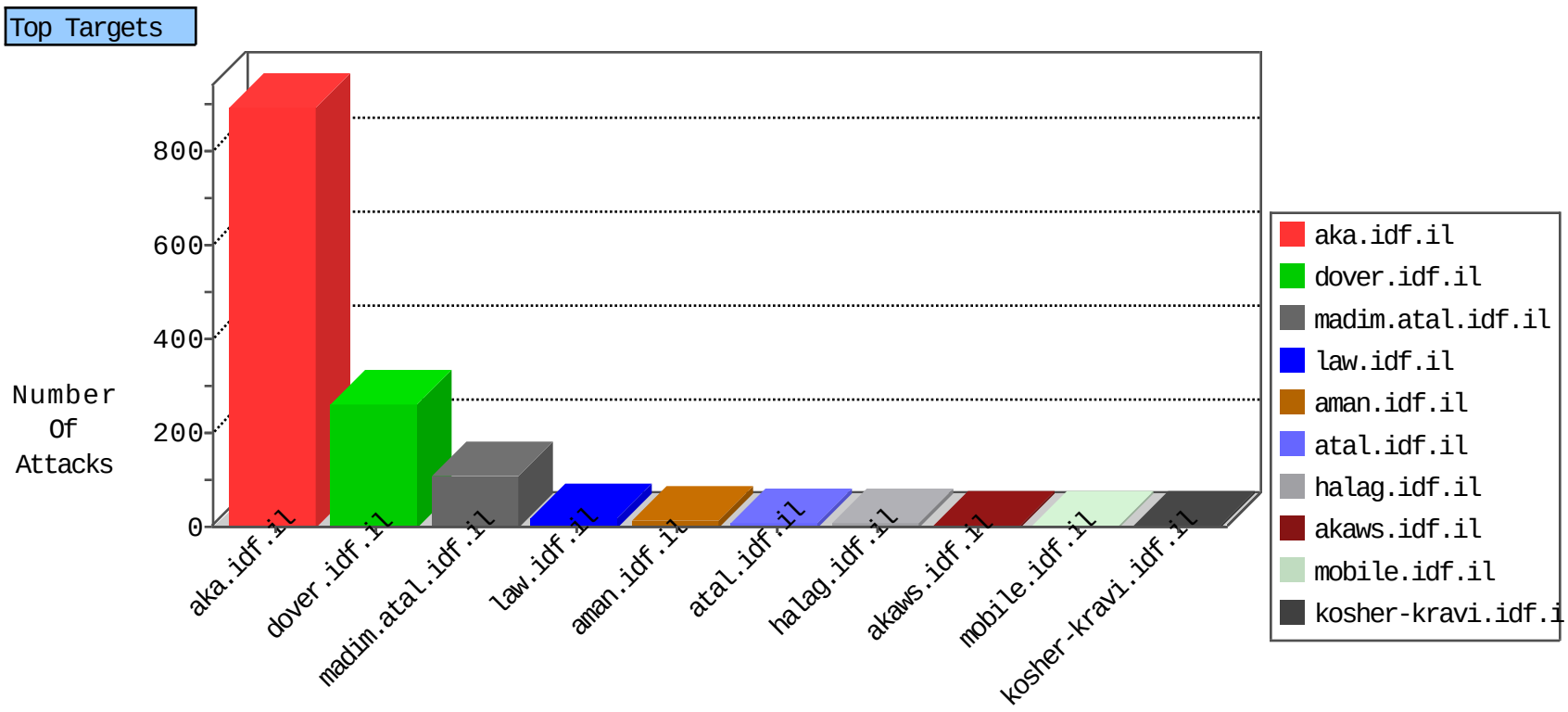
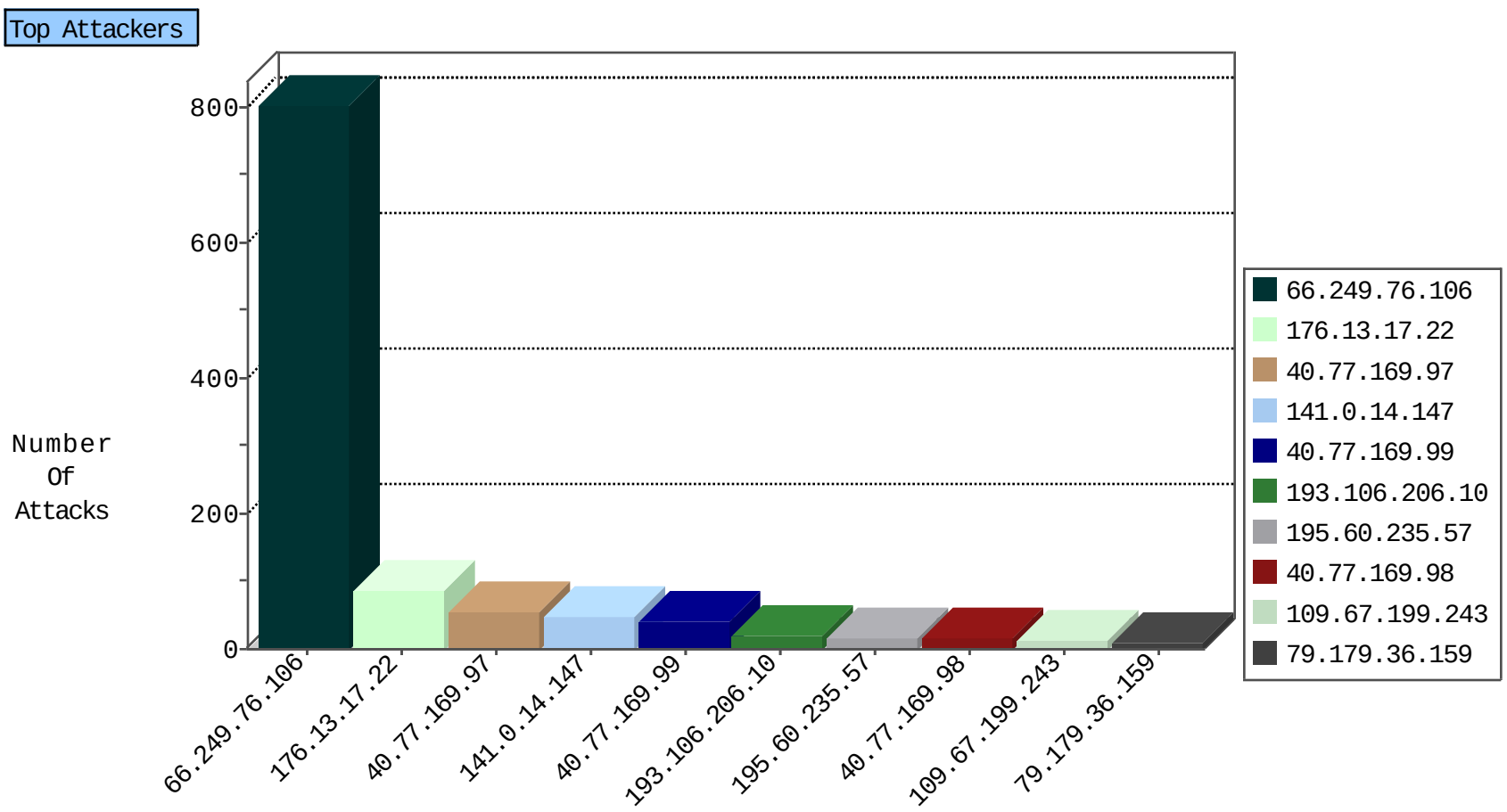
08-23-2016-12:04:05 to 08-23-2016-13:04:05

IDF Under Attack Daily Report



Top Target



Top Attackers

08-23-2016-12:04:05 to 08-23-2016-13:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.19.81	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	14
109.66.12.31	Israel	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	2
209.126.136.2	United States	147.237.76.196	e.sviva.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.34	yohalan.idf.il	Black List	drop	1

08-23-2016-12:04:05 to 08-23-2016-13:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.255.207.28	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
212.47.229.189	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
52.50.60.62	Ireland	147.237.76.86	navy.idf.il	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	1
151.80.31.172	France	147.237.0.15	kosher-kravi.idf.i	C1000146: HTTP: AhrefBot crawler	Block	1
197.2.194.234	Tunisia	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	1

08-23-2016-12:04:05 to 08-23-2016-13:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.76.106	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	804
197.2.194.234	147.237.77.216	Tunisia	dover.idf.il	SQL Injection - Select From	6
79.178.109.155	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
46.116.7.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.0.35	Netherlands	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
45.79.156.96	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
87.236.194.161	147.237.77.178	Czech Republic	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.146.247	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.250.255.76	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.13.78	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.43.162	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.255.90.133	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
2.55.129.234	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.203.77.86	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.124.244.98	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.53.141.222	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.34.160.65	147.237.76.39	Russian Federation	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
77.124.15.67	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
133.242.3.168	147.237.77.179	Japan	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
62.219.48.60	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
95.35.37.153	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.209	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.147.193	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.34.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.183.59	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.65.61.148	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.255.90.133	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.120.19	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.39.222.253	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
202.41.10.3	147.237.77.216	India	dover.idf.il	portscan: TCP Distributed Portscan	1
77.138.168.122	147.237.72.166	France	aka.idf.il	portscan: TCP Distributed Portscan	1
2.55.63.244	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.124.51.14	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
141.226.161.58	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.128.233	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

08-23-2016-12:04:05 to 08-23-2016-13:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.0.14.147	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
40.77.169.99	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	42
40.77.169.97	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	31
193.106.206.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
40.77.169.97	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	15
40.77.169.98	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	13
40.77.169.102	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
40.77.169.97	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	8
109.253.205.61	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	8
62.0.238.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
59.183.183.197	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
40.77.169.100	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	5
182.75.8.110	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
89.237.97.58	France	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
62.0.210.1	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
119.82.112.226	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
176.13.15.149	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
109.66.12.31	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	2
40.77.169.98	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
184.105.139.67	United States	147.237.8.50	e.tikshuv.idf.il	drop	SAM rule	drop	1
109.253.131.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
40.77.169.102	United States	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
109.253.199.165	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.227.173	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
101.178.206.92	Australia	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
139.162.37.113	United States	147.237.0.35	akaws.idf.il	drop		drop	1

08-23-2016-12:04:05 to 08-23-2016-13:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.17.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	86
109.67.199.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
195.60.235.57	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 195.60.235.57	Block	13
79.179.36.159	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	10
40.77.169.103	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	6
80.246.130.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
2.53.18.230	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
81.218.97.45	Israel	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	3
81.218.97.45	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/592-3092-he/	Block	3
66.249.79.37	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
81.218.56.171	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.56.171	Block	3
80.246.130.54	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
31.168.27.216	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 31.168.27.216	Block	2
78.108.164.62	Lebanon	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	2
109.253.136.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.66.58.2	Israel	147.237.72.166	aka.idf.il	Unknown Parameter giyus in aka.idf.il/	None	1
40.77.169.104	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
31.168.27.216	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/4/2094.jpg	Block	1
79.177.10.204	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
195.60.235.57	Israel	147.237.72.166	aka.idf.il	Unknown Parameter nfr in www.aka.idf.il/sip_storage/files/5/68515.gif	None	1
66.102.9.76	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/lomdim/main/	Block	1
140.147.249.7	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/rights/asp/info.asp	Block	1
87.68.33.193	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
40.77.169.103	United States	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
185.32.179.78	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
77.139.51.60	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
46.19.85.131	Israel	147.237.77.233	atal.idf.il	Abnormally Long Request method	Block	1
109.66.58.2	Israel	147.237.72.166	aka.idf.il	Unknown Parameter giyus in aka.idf.il/main/home/default.aspx	None	1
31.168.151.128	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
79.177.217.236	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
195.60.235.57	Israel	147.237.72.166	aka.idf.il	Unknown Parameter nfr in www.aka.idf.il/sip_storage/files/6/68516.gif	None	1
157.55.39.38	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/ãƒâ¢ã¢â€šâ¬ã…â½	Block	1
109.65.12.123	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
40.77.169.103	United States	147.237.77.176	matpash.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
80.246.130.237	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.243.55.130	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
77.139.165.205	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/accepted.aspx	Block	1
46.19.85.131	Israel	147.237.77.233	atal.idf.il	Illegal HTTP Version	Block	1
109.66.58.2	Israel	147.237.72.166	aka.idf.il	Unknown Parameter giyus in www.aka.idf.il/main/home/default.aspx	None	1
32.210.21.183	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	1
82.81.69.86	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
207.46.13.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
157.55.39.140	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.93.82	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
109.65.24.124	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	1
2.55.11.254	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
77.237.146.28	Czech Republic	147.237.77.234	halag.idf.il	Unauthorized URL Access to /	Block	1
46.19.85.131	Israel	147.237.77.233	atal.idf.il	Malformed URL __atuvs=57bc1947cd21100a000	Block	1
82.81.69.86	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/wp-login.php	Block	1
37.26.148.251	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1

08-23-2016-12:04:05 to 08-23-2016-13:04:05