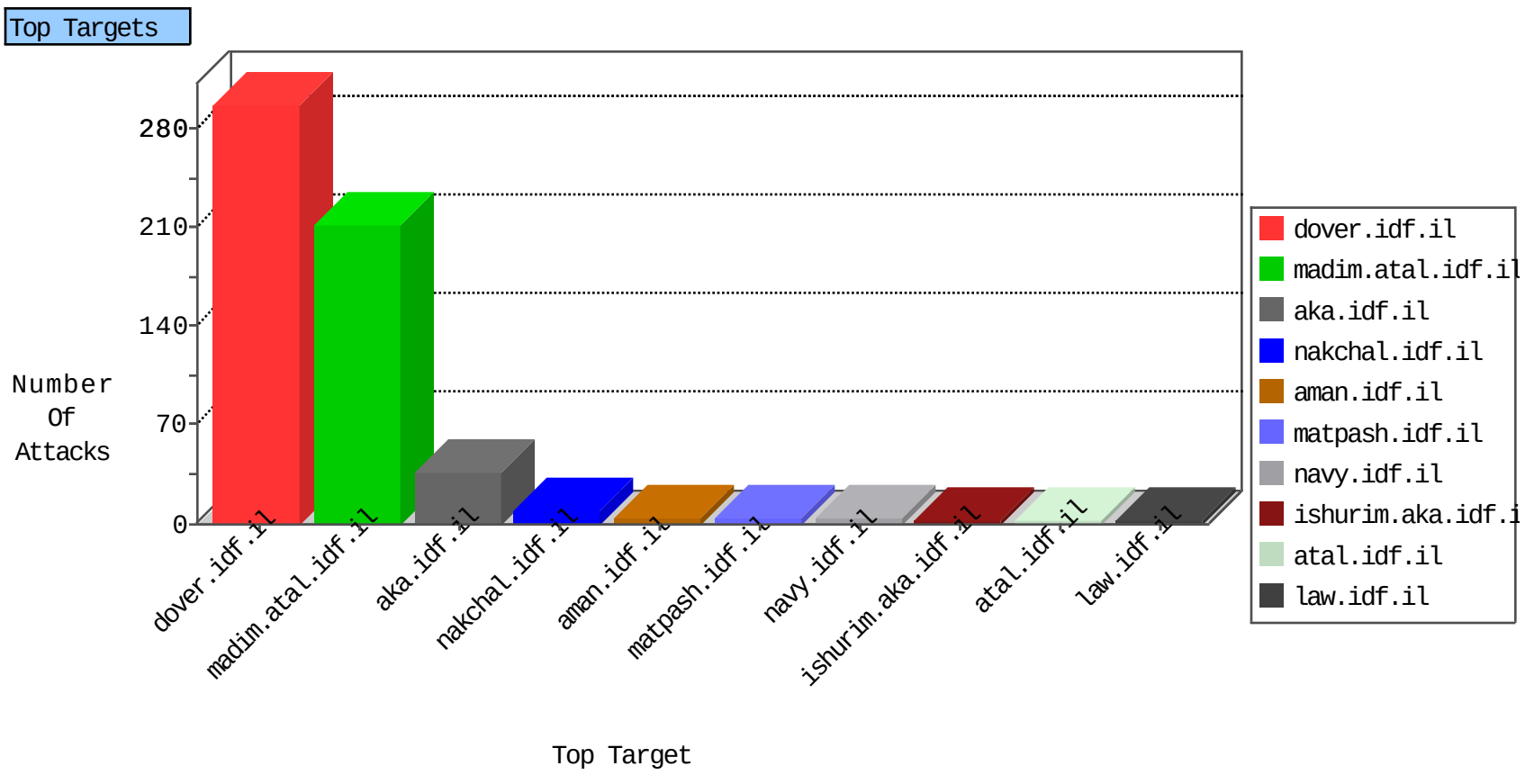
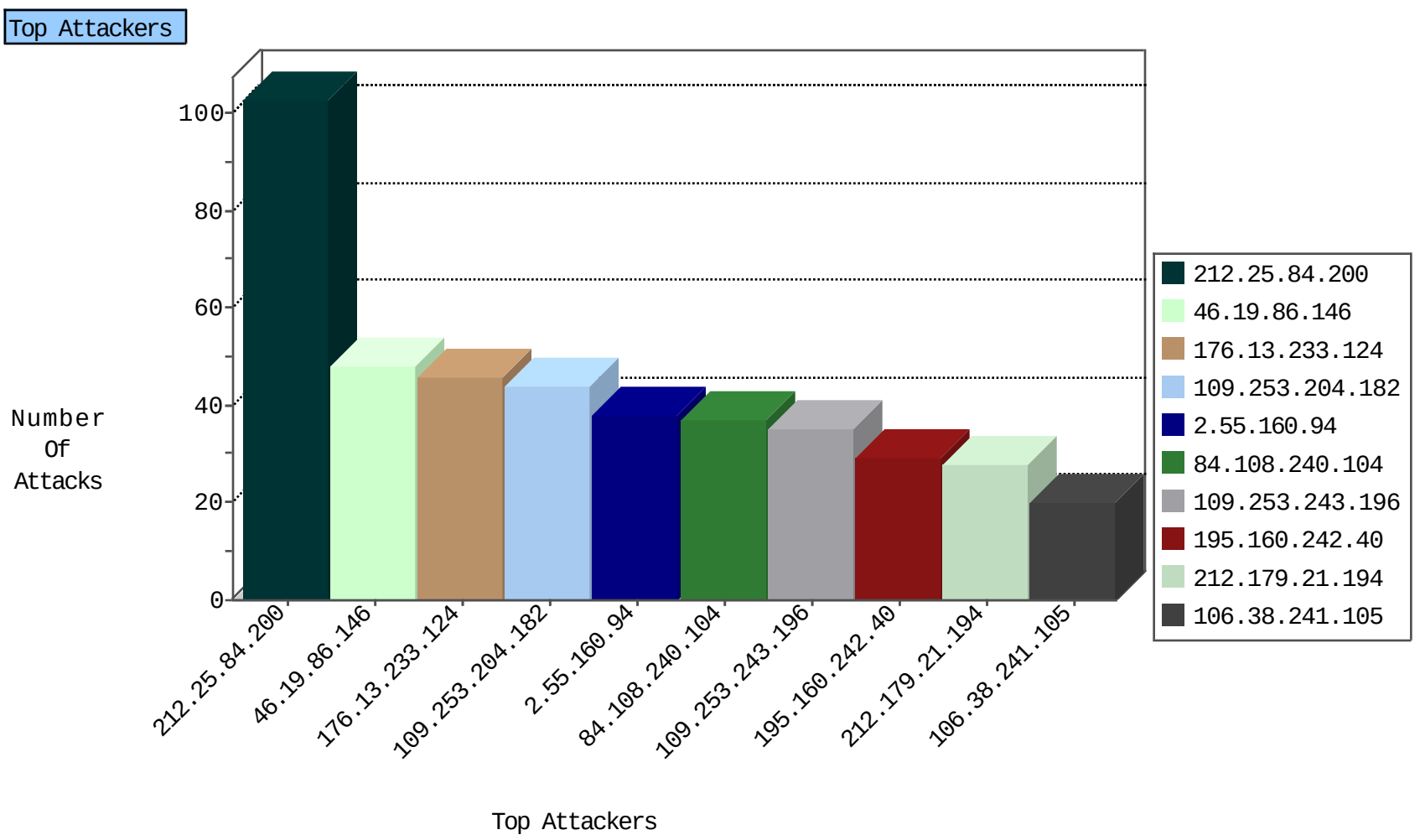
08-17-2016-11:04:05 to 08-17-2016-12:04:05

IDF Under Attack
Daily Report





08-17-2016-11:04:05 to 08-17-2016-12:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.110.148.34	Italy	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	217
82.80.78.2	Israel	147.237.77.176	matpash.idf.il	Black List	drop	3
2.53.132.160	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
93.174.95.106	Netherlands	147.237.76.86	navy.idf.il	Black List	drop	1
58.218.204.245	China	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
93.158.200.118	Netherlands	147.237.76.86	navy.idf.il	Black List	drop	1

08-17-2016-11:04:05 to 08-17-2016-12:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.105	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	20
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	4
62.90.49.25	Israel	147.237.72.156	aman.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
51.255.65.54	France	147.237.76.86	navy.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

08-17-2016-11:04:05 to 08-17-2016-12:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.64.187.83	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	4
54.72.0.55	147.237.77.216	Ireland	dover.idf.il	portscan: TCP Distributed Portscan	2
185.32.176.43	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.193	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.53.129.159	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.125.184.101	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	1
84.94.102.158	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.92.227	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.176.8.118	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.125.9.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.219.250.59	147.237.77.216	United Kingdom	dover.idf.il	portscan: TCP Distributed Portscan	1
46.120.99.176	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.152	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.148.223	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.186.78.78	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.174	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.195	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
2.53.22.17	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.248.168.29	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
82.81.214.102	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.24.106	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.138.52.97	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
188.166.250.140	147.237.76.34	Singapore	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.96	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

08-17-2016-11:04:05 to 08-17-2016-12:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.25.84.200	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	103
109.253.204.182	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	43
195.160.242.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
77.138.52.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
148.251.136.8	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
217.132.101.119	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	5
77.124.24.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.87.114.97	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
128.242.249.13	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
40.77.167.51	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
184.105.139.67	United States	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	1
141.212.122.145	United States	147.237.0.200	m4u.idf.il	drop		drop	1
192.243.55.138	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
109.253.213.241	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.165	United States	147.237.0.33	idf.il	drop		drop	1
124.205.165.165	China	147.237.0.35	akaws.idf.il	drop		drop	1
141.212.122.166	United States	147.237.0.33	idf.il	drop		drop	1
81.204.73.240	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
62.0.200.129	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	1
109.253.147.40	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
2.55.178.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.144	United States	147.237.0.200	m4u.idf.il	drop		drop	1
66.249.64.131	Israel	147.237.0.33	idf.il	drop		drop	1

08-17-2016-11:04:05 to 08-17-2016-12:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.146	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
176.13.233.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
2.55.160.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
84.108.240.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
109.253.243.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
82.102.169.113	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	4
46.19.85.88	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
131.253.27.127	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
132.147.105.126	Singapore	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	2
87.70.40.215	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
109.65.154.6	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.65.154.6	Block	2
192.243.55.131	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58563	Block	1
80.246.139.188	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	Illegal Byte Code Character in Method	Block	1
77.139.140.177	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/giyus	Block	1
192.243.55.138	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/kamlar/klali/default.asp?catid=59830&docid=74040&list=1	Block	1
80.179.9.115	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
192.115.248.2	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
109.66.154.100	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/about/pages/hazonveyeud.aspx	Block	1
192.243.55.133	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.133	Block	1
81.218.40.194	Israel	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/sip_storage/files/3/1773.jpg	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Abnormally Long Request method	Block	1
77.154.204.212	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
54.77.36.68	Ireland	147.237.76.31	nakchal.idf.il	Parameter Type Violation search in www.nakhal.idf.il/1120-he/nakhal.aspx	Block	1
136.243.16.208	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/sites/home/default.asp	Block	1
88.190.87.46	France	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Unsupported Cipher	None	1
199.203.215.1	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/sip_storage/files/	Block	1
80.179.115.198	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
192.198.151.44	Europe	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/ishurim	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	NULL Character in Method ýr[[#8]]ŒÑ#£<¶C[[#28]]î[[#2]]•÷s[[#29]]Ó™ÙÕÕ[[#18]]Ó[[#3]]+#012ŒJ	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
109.253.130.216	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
2.55.178.238	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
192.243.55.133	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/info.asp?moduleid=5&catid=22707&docid=22755	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Illegal Byte Code Character in Method	Block	1
79.180.16.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
62.128.45.253	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	Distributed Malformed URL	Block	1
90.182.178.182	Czech Republic	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/booklets.aspx	Block	1
212.179.1.218	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
80.246.133.110	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/size100x0/2970.jpg	Block	1
192.243.55.130	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/www.tikshuv.idf.il	Block	1
169.229.3.91	United States	147.237.0.19	madim.atal.idf.il	NULL Character in Query String on -d•£b¯	Block	1
68.180.229.116	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1073-he/nakhal.aspx	Block	1
192.243.55.138	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	1
79.180.16.20	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-login.php	Block	1
176.13.231.104	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	1
66.102.9.95	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

08-17-2016-11:04:05 to 08-17-2016-12:04:05