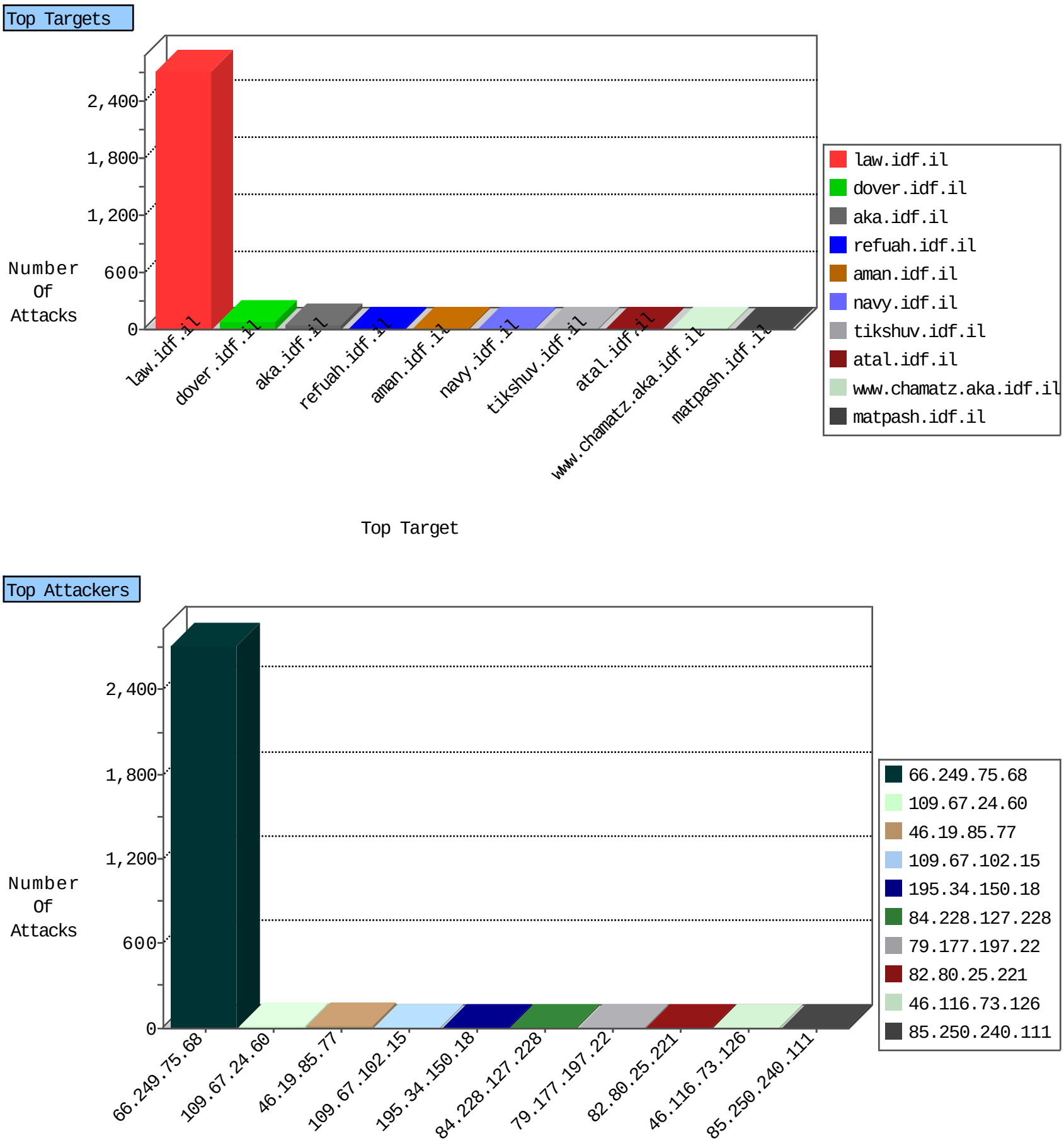
04-25-2015-16:03:01 to 04-25-2015-17:03:01

IDF Under Attack
04-25-2015-16:03:01



04-25-2015-16:03:01 to 04-25-2015-17:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
84.228.127.228	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	121
46.19.85.77	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	80
82.145.217.104	Europe	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
219.126.55.115	Japan	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
37.201.194.12	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
84.229.28.186	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-25-2015-16:03:01 to 04-25-2015-17:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
198.20.70.114	United States	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
79.177.180.3	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
105.154.88.90	Morocco	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
80.178.28.251	Israel	147.237.77.233	atal.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.77.205	prisha.idf.il	DVRep_B-N_60_100	Block	1
84.229.31.182	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.70.114	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.66	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.43.94	Germany	147.237.76.198	e.yohalan.idf.il	DVRep_B-N_60_100	Block	1

04-25-2015-16:03:01 to 04-25-2015-17:03:01

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
66.249.75.68	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2718
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
79.177.197.22	Israel	147.237.0.34	tikshuv.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
2.54.53.139	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
43.255.191.162	Japan	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
188.95.158.198	Ukraine	147.237.8.27	e.madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
109.253.142.43	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
61.183.128.6	China	147.237.8.14	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.162	Japan	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
114.112.96.133	China	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
91.217.90.49	Ukraine	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.77.235	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
61.160.224.130	China	147.237.8.27	e.madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

04-25-2015-16:03:01 to 04-25-2015-17:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
46.19.85.77	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
109.67.102.15	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	monitor	6
85.250.240.111	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.116.73.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
79.181.147.201	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
32.218.38.71	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
157.55.39.59	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
46.230.88.142	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.19.85.34	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
109.67.102.15	Israel	147.237.76.42	refuah.idf.il	SYN retransmit with different window scale	Bad TCP sequence	alert	2
109.65.209.155	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
185.26.182.35	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
80.246.130.246	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
54.82.48.78	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
199.30.25.193	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
207.46.13.1	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
89.138.27.103	Israel	147.237.72.167	ishurim.aka.idf.i	Invalid checksum. Packet dropped.	Streaming Engine: TCP Invalid Checksum	drop	1
46.19.86.253	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
140.139.231.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
69.175.127.10	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1

04-25-2015-16:03:01 to 04-25-2015-17:03:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.67.24.60	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.67.24.60	Block	16
109.67.59.253	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
66.249.73.193	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.193	Block	2
66.249.73.201	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.201	Block	2
176.10.104.227	Switzerland	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 176.10.104.227	Block	2
91.200.12.14	Ukraine	147.237.77.176	matpash.idf.il	PHP Attempt	Block	2
93.172.169.104	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
46.120.187.168	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
157.55.39.5	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
95.173.190.6	Turkey	147.237.77.226	www.chamatz.aka.idf.il	Illegal HTTP Version	Block	1
79.181.99.3	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ScriptManager1_HiddenField in www.aka.idf.il/main/kapatz/citizencontact.aspx	None	1
212.199.218.246	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
31.168.68.51	Israel	147.237.72.166	aka.idf.il	Unknown Parameter q861 in www.aka.idf.il/main/giyus/login.aspx	None	1
89.138.19.235	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
176.12.141.186	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.204	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
46.121.95.36	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.67.24.60	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request URL	Block	1
80.178.28.251	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
213.57.112.207	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 213.57.112.207	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in www.aka.idf.il/chamatz/miktzoa/default.asp	None	1
109.67.102.15	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
37.26.146.230	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
89.145.95.2	United Kingdom	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/894-he/refuah.aspx	Block	1
176.12.151.122	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.69.70	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/...	Block	1
109.67.24.60	Israel	147.237.72.166	aka.idf.il	Illegal URL Path Encoding www.aka.idf.il/main/giyus/function () { var c = math.round(this[2] / 100 * 255); if (this[1] == 0) { return [c, c, c]; } else { var a = this[0] r 360; var e = a e 60; var g = math.round((this[2] * (100 - this[1])) / 10000 * 255); var d = math.round((this[2] * (6000 - this[1] * e)) / 600000 * 255); var b = math.round((this[2] * (6000 - this[1] * (60 - e))) / 600000 * 255); switch (math.floor(a / 60)) { case 0: return [c, b, g];	Block	1
80.246.133.202	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
213.57.112.207	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/8/	Block	1
66.249.75.54	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
37.201.194.12	Germany	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
125.65.46.140	China	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	1
66.249.79.112	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/m/	Block	1
198.20.69.74	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
66.249.69.76	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
157.55.39.39	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
5.29.219.229	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1
84.110.8.22	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//https:/www.aka.idf.il/	Block	1
176.10.104.227	Switzerland	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/900-he/	Block	1
66.249.78.4	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1401-he/atal.aspx	Block	1
46.19.86.227	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
149.78.197.11	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/trajector/	Block	1
207.46.13.52	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
157.55.39.89	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.73.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.185	Block	1

04-25-2015-16:03:01 to 04-25-2015-17:03:01