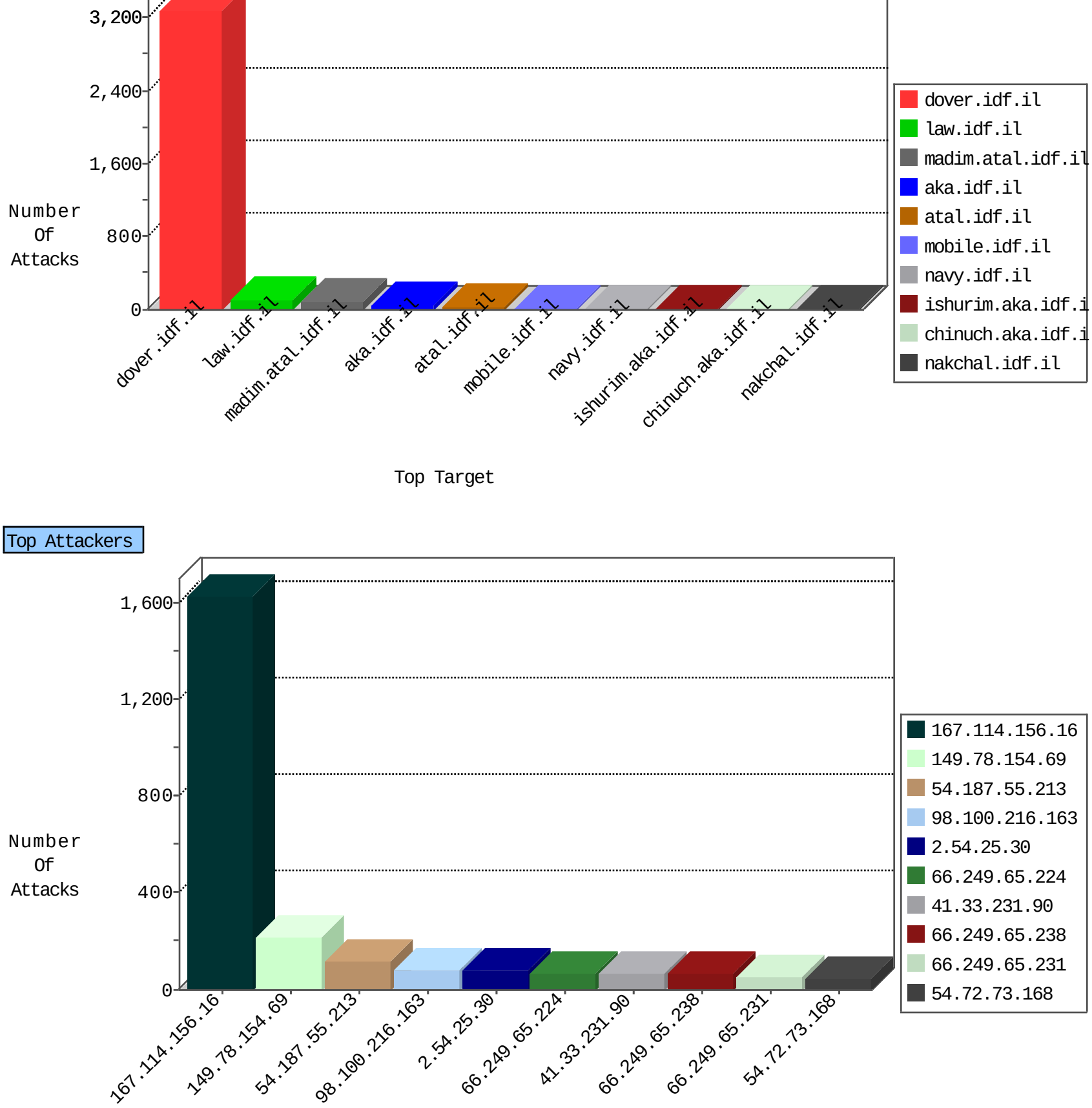
11-07-2015-01:04:09 to 11-07-2015-02:04:09

IDF Under Attack Daily Report



11-07-2015-01:04:09 to 11-07-2015-02:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2861
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	446
37.26.149.138	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	85
5.22.129.140	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	11
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	6
5.22.129.140	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	5
134.147.203.115	Germany	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	4
54.244.22.103	United States	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
134.147.203.115	Germany	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	2
222.186.34.48	China	147.237.76.31	nakchal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
213.176.236.128	Russian Federation	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

11-07-2015-01:04:09 to 11-07-2015-02:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
98.100.216.163	United States	147.237.77.74	law.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	20
165.215.209.15	United States	147.237.77.216	dover.idf.il	14511: HTTP: Win32/Oliga Fake User Agent	Block	1

11-07-2015-01:04:09 to 11-07-2015-02:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
98.100.216.163	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	60
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.6	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
104.192.0.20	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.160.155	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
80.40.134.103	147.237.77.216	United Kingdom	dover.idf.il	portscan: TCP Distributed Portscan	1
188.138.9.51	147.237.76.31	Germany	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
104.192.0.20	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.174.106	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.8	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1

11-07-2015-01:04:09 to 11-07-2015-02:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	214
54.187.55.213	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	116
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	44
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
66.249.65.238	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	38
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	36
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
66.249.65.231	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
188.165.15.14	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
37.46.174.171	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
46.19.85.214	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
66.249.65.224	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
87.69.7.151	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
2.52.31.93	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
73.22.155.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
213.57.250.97	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
24.114.24.245	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
66.249.65.231	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
66.249.65.238	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
188.247.77.181	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
17.142.152.72	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
66.249.65.238	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
183.79.221.13	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
17.142.152.86	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
176.12.136.173	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.65.214.133	Israel	147.237.77.243	mobile.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
17.142.152.81	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
17.142.156.109	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.100.123.141		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
41.34.189.131	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
80.246.130.61	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
17.142.152.110	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.181.5.146	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
80.43.229.86	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
149.78.72.163	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
66.249.65.231	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
80.246.133.170	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
82.80.25.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
79.178.191.239	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
5.22.129.140	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.139.108.248	Spain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.26.149.138	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.25.30	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.25.30	Block	61
2.54.25.30	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	19
208.115.111.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	2
73.22.155.10	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
109.65.214.133	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
73.22.155.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/	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
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/size100x0/3350.jpg	Block	1
174.116.25.68	Canada	147.237.77.74	law.idf.il	Illegal Byte Code Character in Method _[[#0]][[#0]][[#0]]DÂ¢ZÃ‡Â‰Ã^aÃš [[#1]][[#12]]i$b+Ã¿?n2")Ã?Ã?J[[#12]]=Â±Ãƒ[[#17]]G,'[[#30]]Â€ÂŽÂƒÂ” N:7ÃƒÃ•{	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unknown Parameter gt; in www.aka.idf.il/main/rabanut/general.aspx	None	1
174.116.25.68	Canada	147.237.77.74	law.idf.il	Unknown HTTP Request Method _[[#0]][[#0]][[#0]]DÂ¢ZÃ‡Â‰Ã^aÃš [[#1]][[#12]]i$b+Ã¿?n2")Ã?Ã?J[[#12]]=Â±Ãƒ[[#17]]G,'[[#30]]Â€ÂŽÂƒÂ” N:7ÃƒÃ•{ in URL	Block	1
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/7/63577.doc	Block	1
66.249.64.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/size100x0/3493.jpg	Block	1
174.116.25.68	Canada	147.237.77.74	law.idf.il	Malformed URL	Block	1
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
183.79.221.13	Japan	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
31.154.145.255	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.248	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/civiladministration/matak/pages/economy.aspx	Block	1
66.249.78.4	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/894-he/atal.aspx	Block	1
66.249.64.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/size100x0/3250.jpg	Block	1
174.116.25.68	Canada	147.237.77.74	law.idf.il	NULL Character in Header Name at	Block	1
79.178.203.221	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/recruitlane.aspx	Block	1
66.249.67.90	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/894-en	Block	1
37.239.151.130	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
183.79.223.85	Japan	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
174.116.25.68	Canada	147.237.77.74	law.idf.il	Abnormally Long Request method	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.153	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/sip_storage/files/8/638.pds	Block	1
174.116.25.68	Canada	147.237.77.74	law.idf.il	NULL Character in Method _[[#0]][[#0]][[#0]]DÂ¢ZÃ‡Â‰Ã^aÃš [[#1]][[#12]]i$b+Ã¿?n2")Ã?Ã?J[[#12]]=Â±Ãƒ[[#17]]G,'[[#30]]Â€ÂŽÂƒÂ” N:7ÃƒÃ•{	Block	1
80.246.130.61	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
62.210.88.201	France	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 51.254.206.142/httptest.php	Block	1
207.46.13.71	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/english	Block	1
174.116.25.68	Canada	147.237.77.74	law.idf.il	Illegal Byte Code Character in Header Name	Block	1
66.249.64.186	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
174.116.25.68	Canada	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
84.109.44.72	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	1

11-07-2015-01:04:09 to 11-07-2015-02:04:09