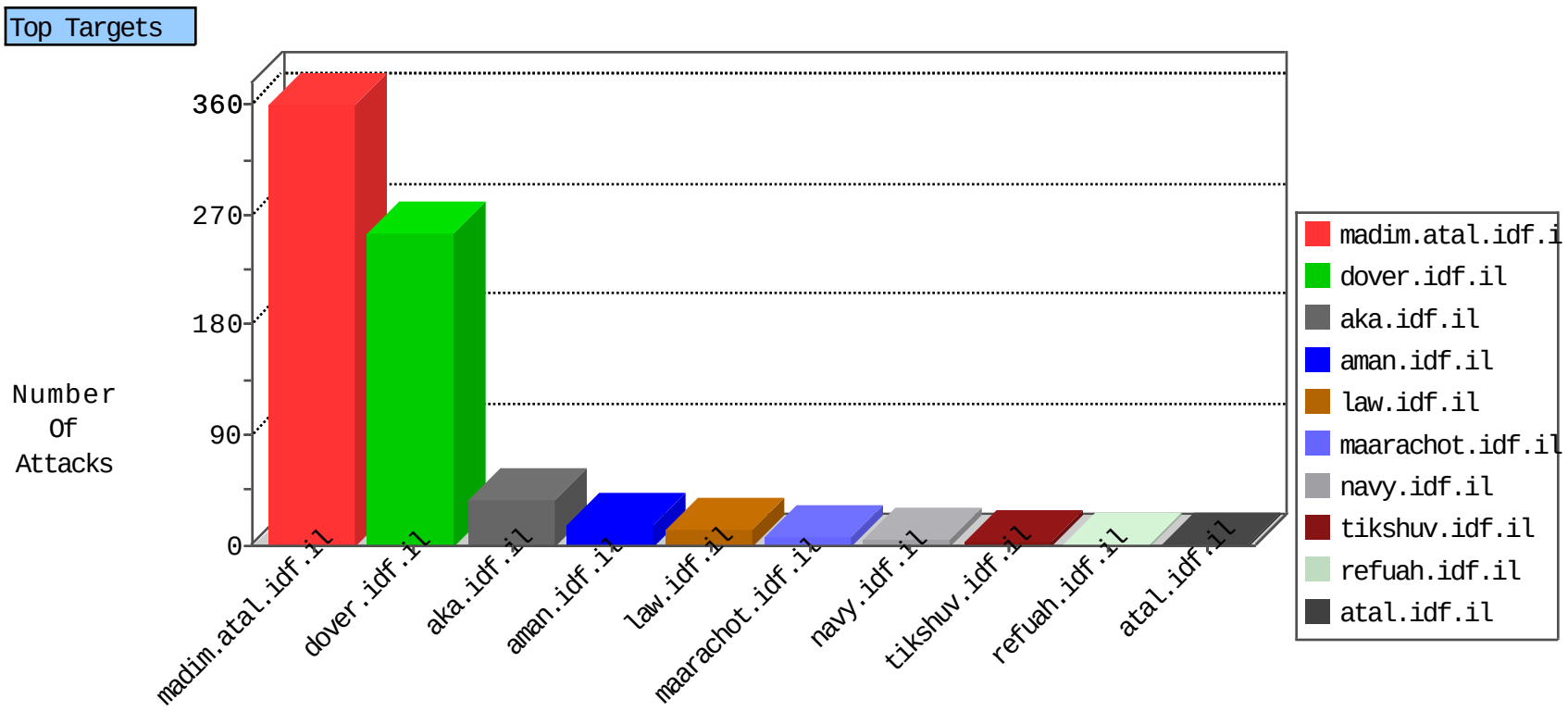
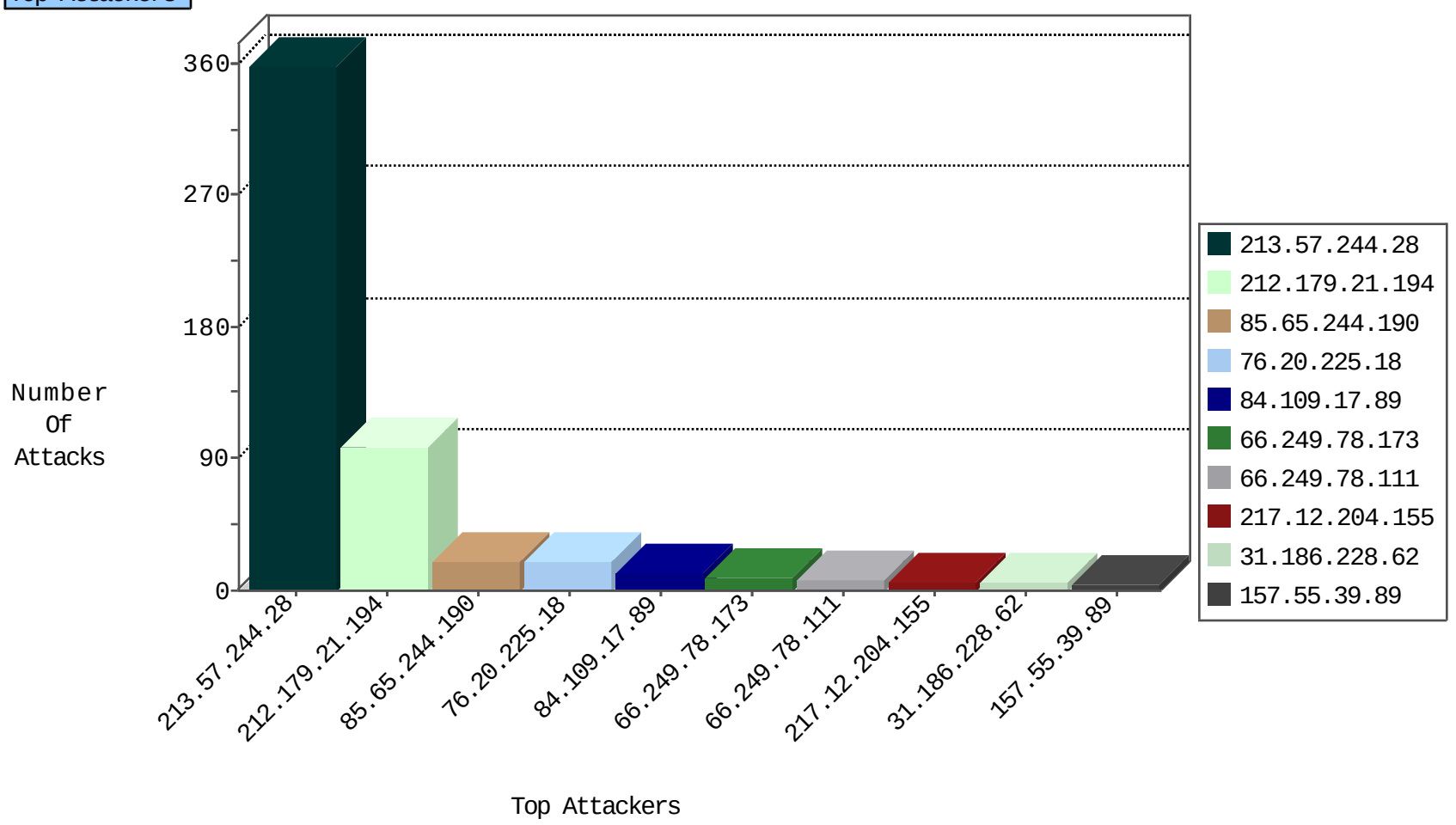
04-25-2015-18:03:00 to 04-25-2015-19:03:00

IDF Under Attack
04-25-2015-18:03:00

Top Targets



Top Attackers



04-25-2015-18:03:00 to 04-25-2015-19:03:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
66.249.78.15	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	3244
84.109.17.89	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	82
46.116.68.205	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	60
109.66.37.213	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	53
66.249.78.111	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	33
77.91.220.76	Sweden	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5
66.249.78.173	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
218.3.243.223	China	147.237.76.197	e.himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	1

04-25-2015-18:03:00 to 04-25-2015-19:03:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
176.228.56.240	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
198.20.69.98	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
199.168.141.77	United States	147.237.77.216	dover.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	1
37.142.198.44	Israel	147.237.76.42	refuah.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

04-25-2015-18:03:00 to 04-25-2015-19:03:00

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.78.15	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sA (2)	2
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
58.20.54.249	China	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
87.229.10.80	Hungary	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.242.17	Russian Federation	147.237.77.216	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
87.229.10.80	Hungary	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1

04-25-2015-18:03:00 to 04-25-2015-19:03:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
212.179.21.194	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	98
85.65.244.190	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
76.20.225.18	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	20
31.186.228.62	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
31.186.228.61	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
31.186.228.92	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
87.69.106.212	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
87.69.128.159	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
109.64.96.160	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
31.186.228.29	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
31.186.228.93	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
31.186.228.94	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
46.19.85.186	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	alert	3
207.46.13.52	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
31.186.228.27	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
77.127.216.92	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.117.84.153	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
109.65.29.102	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.121.16.29	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.19.86.15	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
109.66.127.53	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
31.186.228.32	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
79.181.6.232	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
31.186.228.67	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.19.86.234	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
37.26.146.250	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
31.186.228.59	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
84.229.208.249	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
31.186.228.90	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
109.253.136.67	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
46.19.85.186	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
78.145.24.234	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
37.201.194.12	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
109.253.137.168	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
68.180.228.224	United States	147.237.0.15	kosher-kravi.idf.il	SAM rule	drop	drop	1
46.19.85.209	Israel	147.237.77.176	matpash.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
109.65.96.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
31.186.228.30	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
79.176.104.221	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
109.253.144.72	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
31.186.228.66	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
60.242.18.20	Australia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
41.33.232.65	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
128.242.249.13	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
92.239.236.232	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
31.186.228.25	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
213.57.244.28	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 213.57.244.28	Block	358
217.12.204.155	Ukraine	147.237.77.74	law.idf.il	PHP Attempt	Block	6
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	4
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
84.111.80.113	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.5	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
87.69.194.53	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
77.127.231.70	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
109.226.60.187	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 109.226.60.187	Block	1
58.57.200.34	China	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to 147.237.0.19/cgi-bin/php5-cli	Block	1
84.109.209.166	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
199.168.141.77	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ckeditor/ckfinder/core/connector/asp/connector.asp	Block	1
176.12.139.163	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.167	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.5	United States	147.237.72.166	aka.idf.il	Unknown Parameter pagenum in aka.idf.il/kamlar/news/	None	1
66.249.78.96	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
46.116.138.219	Israel	147.237.72.166	aka.idf.il	Double URL Encoding - parameter: url in aka.idf.il/main/giyus/general.aspx	Block	1
91.200.12.22	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-11845-en/dover.aspx/trackback/	Block	1
188.165.15.94	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1
79.183.115.237	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il//himush/site/he/himush.asp	Block	1
157.55.39.89	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/chamatz/general/default.asp	None	1
109.226.60.187	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/templates/oprolescategory/oprolescategory.aspx	Block	1
58.57.200.34	China	147.237.0.34	tikshuv.idf.il	Access to: /cgi-bin/php5-cli	Block	1
84.111.15.106	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
207.46.13.95	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/french/idf_in_pictures/2003/january/26.stm	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/armored/barak/kkkkkkk=258f21cakkkkkkk_258f21ca	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
46.116.240.50	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
109.67.184.189	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
80.246.133.10	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
190.213.250.121	Trinidad and Tobago	147.237.72.166	aka.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
157.55.39.115	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
132.76.40.102	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.69.40	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1
213.57.244.28	Israel	147.237.0.19	madim.atal.idf.i	Too Many 404: Response Code per Session	Block	1
180.76.4.152	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
77.127.194.142	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/fr.hamas	Block	1
157.55.39.89	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
52.6.31.228	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-6596-he/	Block	1
109.160.141.92	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
84.95.123.79	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
199.168.141.77	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 199.168.141.77	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/images/0108	Block	1
157.55.39.178	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.3	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.78.22	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
5.79.73.246	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.stm	Block	1

04-25-2015-18:03:00 to 04-25-2015-19:03:00