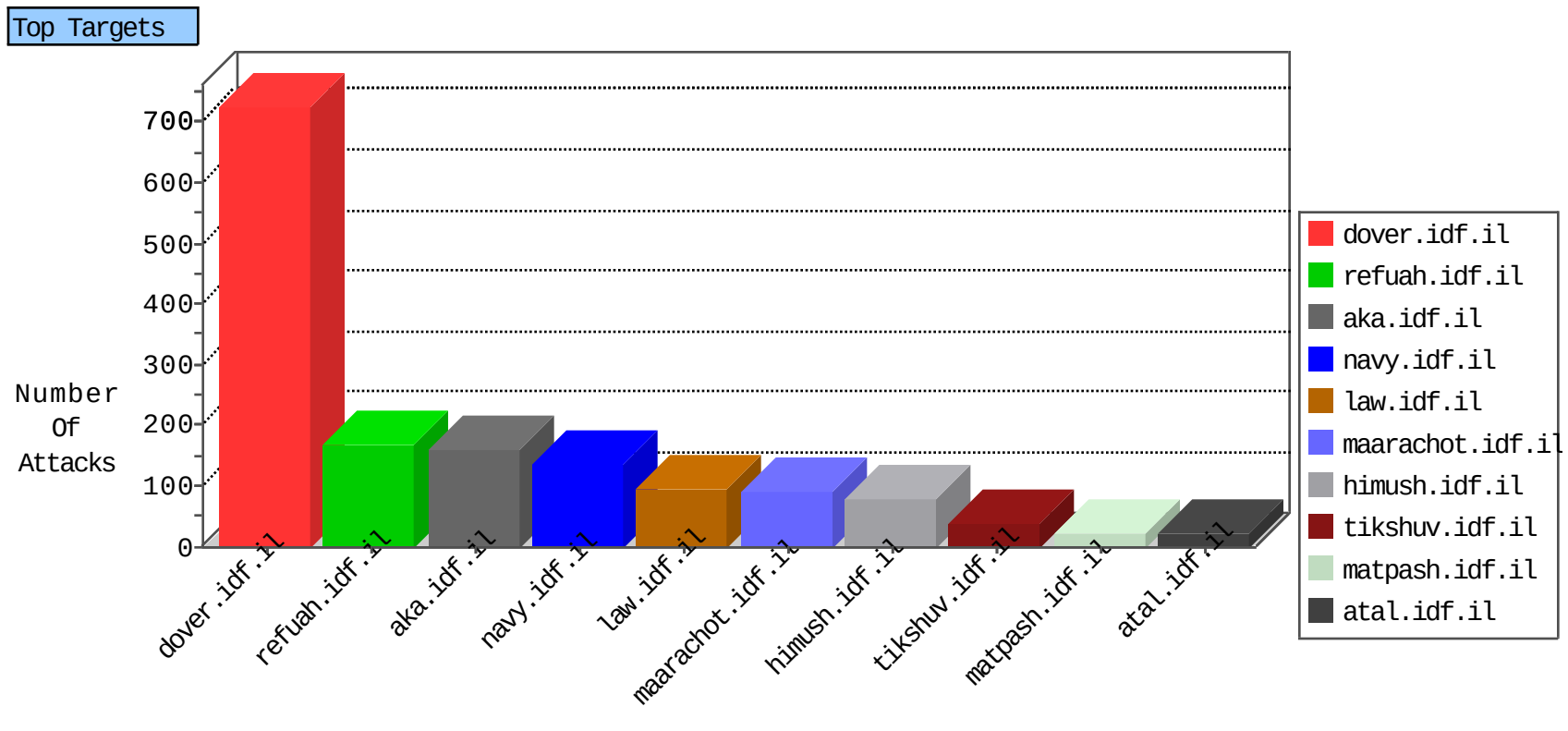
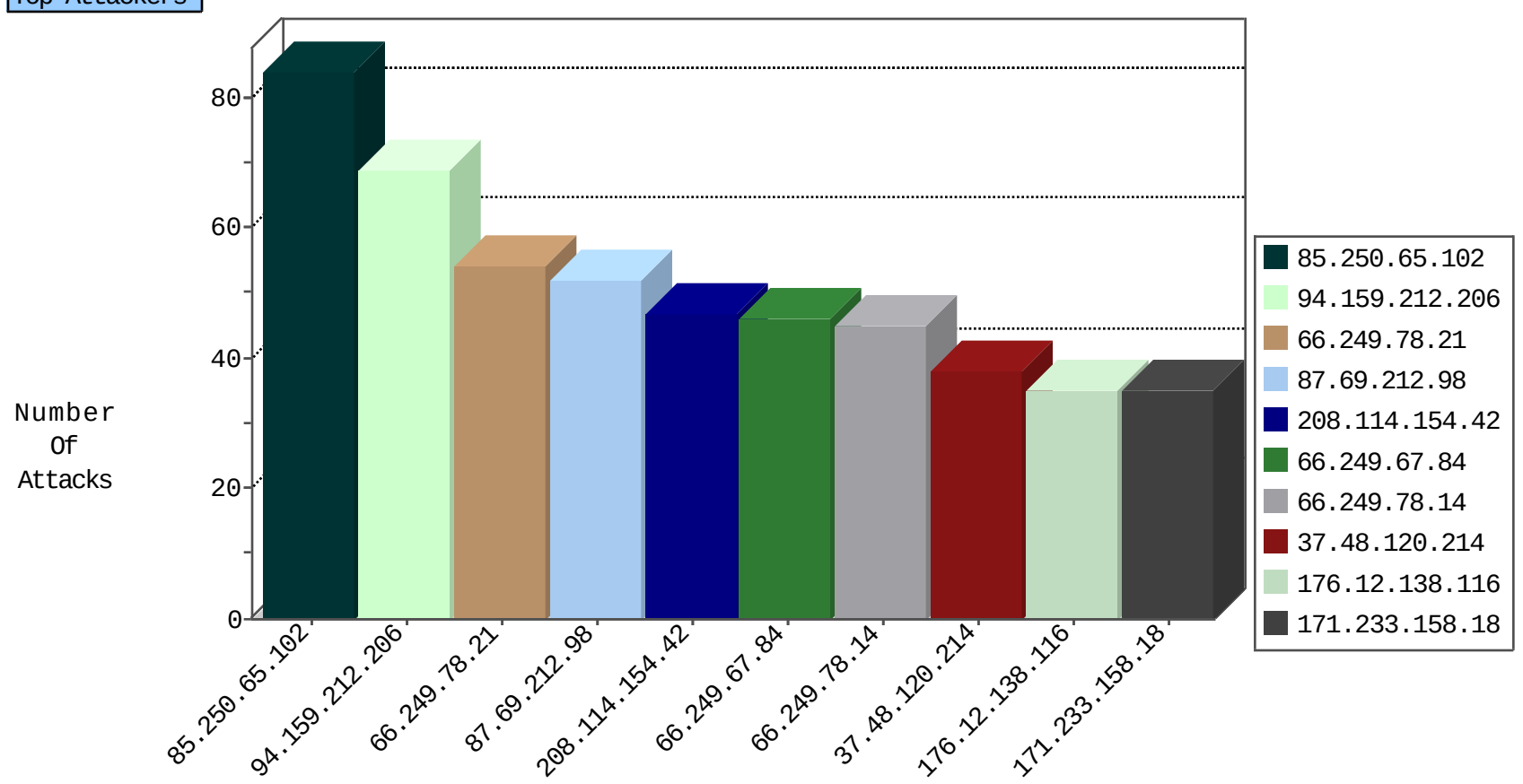
04-12-2015-02:03:08 to 04-12-2015-03:03:08

IDF Under Attack
04-12-2015-02:03:08

Top Targets



Top Attackers



04-12-2015-02:03:08 to 04-12-2015-03:03:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.112	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	220
66.249.78.21	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	54
66.249.67.84	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	46
66.249.78.14	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	45
220.181.108.79	China	147.237.76.86	navy.idf.il	TCP handshake violation, first packet not syn	drop	36
66.249.69.101	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	33
66.249.67.107	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	33
66.249.64.132	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	31
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	29
66.249.64.136	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	26
66.249.69.109	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	25
66.249.67.115	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	24
66.249.67.76	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	23
66.249.67.92	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	21
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	20
66.249.67.99	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	20
66.249.78.160	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	17
66.249.67.14	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	15
66.249.78.28	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	15
66.249.69.93	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	15
66.249.69.42	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	14
66.249.78.174	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	14
66.249.78.190	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	13
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	13
66.249.89.97	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	12
66.249.69.50	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	11
66.249.93.239	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	11
66.249.69.34	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	10
66.249.78.248	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	9
66.249.78.167	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	9
66.249.67.30	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	8
66.249.64.128	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	8
66.249.67.22	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	7
66.249.81.209	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	7
66.249.64.155	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	6
82.145.222.80	Europe	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	6
66.249.78.93	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	6
94.159.212.206	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
66.249.93.168	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6
66.249.67.155	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	5
66.249.81.198	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	5
66.249.67.116	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	5
66.249.78.95	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
66.249.89.93	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	4
66.249.93.160	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4
66.249.78.197	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	4
66.249.64.150	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	4
66.249.79.24	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	4
66.249.78.204	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	4

04-12-2015-02:03:08 to 04-12-2015-03:03:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
180.76.5.193	China	147.237.0.34	tikshuv.idf.il	DVRep_P-N_40-59	Permit	29
89.139.185.104	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4

04-12-2015-02:03:08 to 04-12-2015-03:03:08

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	6
132.68.245.243	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	3
109.65.6.99	Israel	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	2
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
221.235.188.212	China	147.237.77.176	matpash.idf.il	ET SCAN Potential SSH Scan	1
113.108.246.42	China	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
113.108.246.42	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
91.224.132.118	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.27.204.27	China	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
124.124.197.27	India	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
113.108.246.42	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.76.148	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	China	147.237.76.31	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.188.212	China	147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
221.235.188.212	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
124.124.197.27	India	147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 4096	1

04-12-2015-02:03:08 to 04-12-2015-03:03:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
94.159.212.206	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	65
85.250.65.102	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	monitor	53
87.69.212.98	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	52
208.114.154.42	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	47
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	38
176.12.138.116	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
171.233.158.18	Vietnam	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	35
85.250.65.102	Israel	147.237.76.86	navy.idf.il	Invalid ACK number	Bad TCP sequence	alert	31
95.86.104.233	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	24
46.120.173.130	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	16
96.40.153.231	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
99.240.83.69	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	13
109.253.140.82	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
17.142.151.101	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
17.142.152.68	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
89.139.185.104	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
82.145.222.80	Europe	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
195.154.235.127	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
17.142.152.111	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
17.142.145.3	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
17.142.152.89	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
204.237.22.235	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
207.46.13.82	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
184.173.183.173	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
79.179.125.25	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
84.228.144.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
199.30.24.36	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
82.80.25.221	Israel	147.237.77.216	dover.idf.il	SAM rule	drop	drop	4
207.241.237.208	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
37.26.148.172	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
17.142.152.110	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
207.241.237.208	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
157.55.39.171	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
17.142.152.85	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
37.26.147.242	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
77.125.73.12	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
79.181.155.227	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
46.19.86.64	Israel	147.237.77.243	mobile.idf.i	Invalid ACK number	Bad TCP sequence	monitor	3
109.186.7.160	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
207.161.165.210	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
80.246.130.16	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
109.186.7.160	Israel	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	3
2.52.41.157	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
70.190.60.243	United States	147.237.77.234	halag.idf.il	SAM rule	drop	drop	2

04-12-2015-02:03:08 to 04-12-2015-03:03:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.67.117.232	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	6
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
109.67.117.232	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 109.67.117.232	Block	2
176.12.139.231	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	2
157.55.39.171	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
157.55.39.172	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
207.46.13.82	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/121003-1.stm	Block	1
155.133.18.153	Poland	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
37.142.1.232	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.12.137.150	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
52.4.217.116	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
157.55.39.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/homefront/english/ie-index.stm	Block	1
79.176.203.192	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
37.142.171.37	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
176.12.139.157	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/haredim/webresource.axd	Block	1
54.172.196.207	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
157.55.39.114	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/info05.stm	Block	1
79.181.181.202	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.85.6	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
149.78.187.214	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
69.12.75.115	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-10578-en/dover.aspx/rk=0/rs=iapj4ki6d6lbmvw8fvoa4zejeke-	Block	1
85.64.20.219	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
46.19.123.125	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
188.165.15.241	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/0112-1.stm	Block	1
155.133.18.153	Poland	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1
70.190.60.243	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
37.26.147.210	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.64.123.175	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
46.245.139.138	Greece	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/0218-3.stm	Block	1

04-12-2015-02:03:08 to 04-12-2015-03:03:08