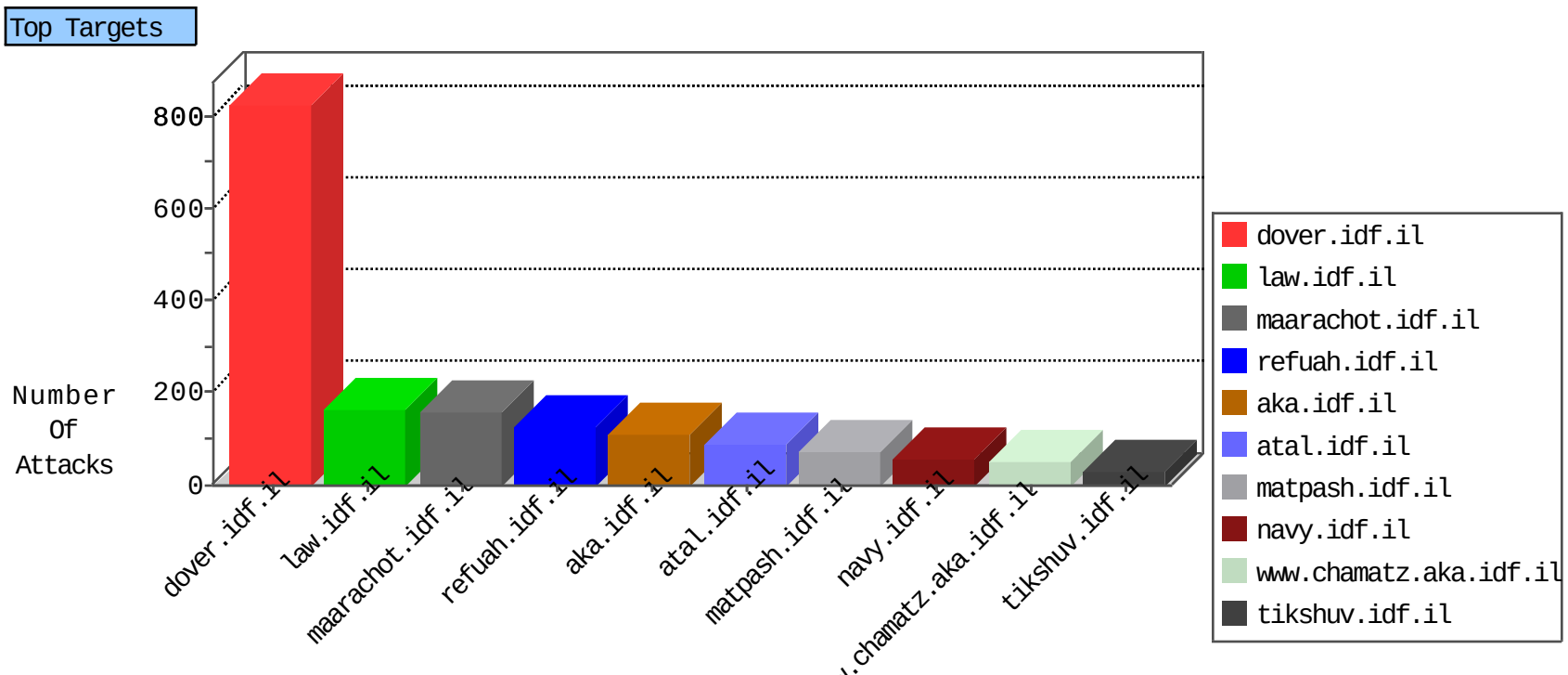
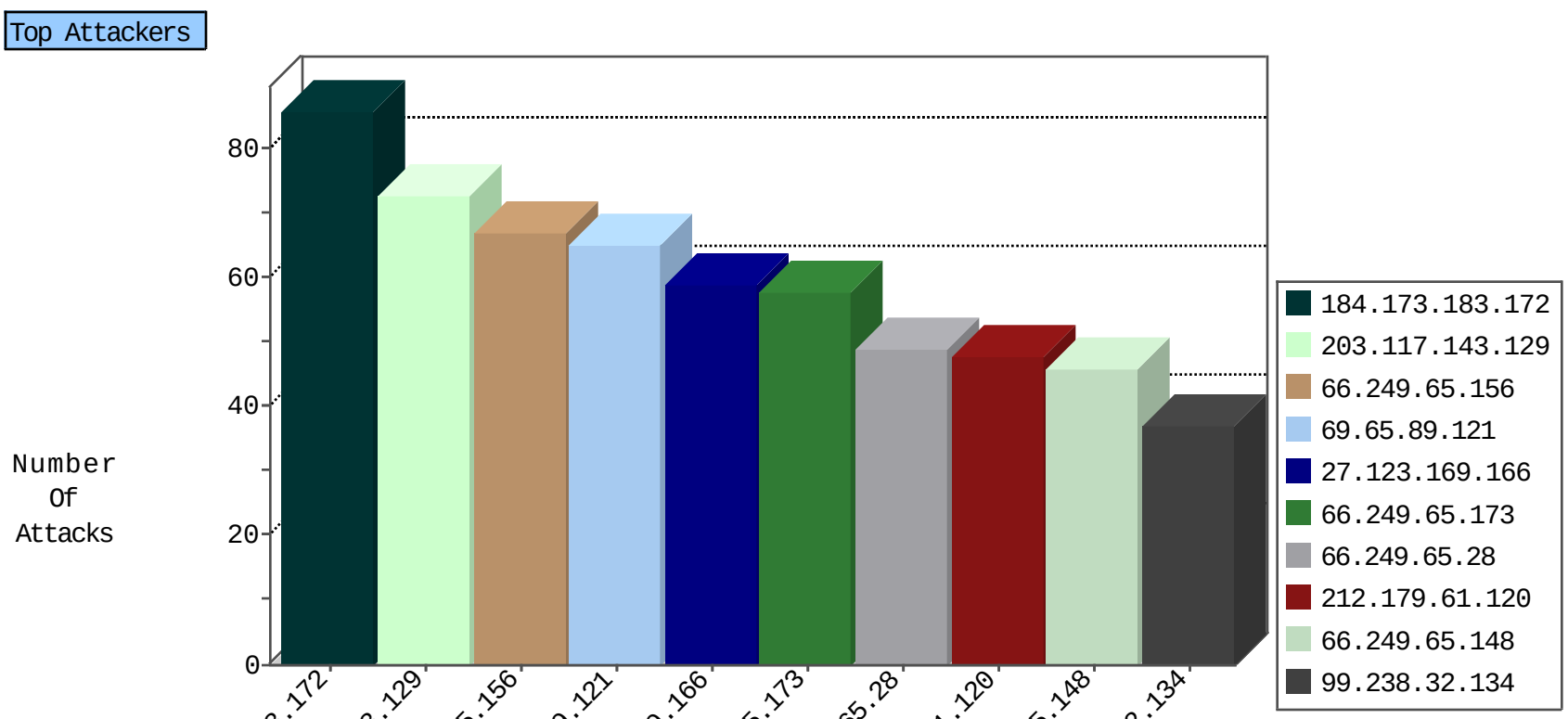
04-14-2015-05:03:08 to 04-14-2015-06:03:08

IDF Under Attack
04-14-2015-05:03:08

Top Targets



Top Attackers



04-14-2015-05:03:08 to 04-14-2015-06:03:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.156	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	79
66.249.65.156	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	66
66.249.65.173	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	58
66.249.65.28	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	49
66.249.65.148	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	46
66.249.73.219	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	34
66.249.65.152	United States	147.237.77.170	maarachot.idf.il	Block_Ip_Web_In	drop	32
66.249.65.3	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	26
66.249.65.181	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	26
66.249.65.52	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	25
66.249.73.203	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	24
66.249.65.177	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	24
66.249.65.39	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	23
66.249.65.10	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	23
66.249.73.201	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	21
66.249.65.44	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	19
66.249.65.26	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	18
66.249.78.159	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	17
66.249.73.217	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	17
66.249.78.166	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	17
66.249.73.211	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	16
66.249.65.30	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	16
66.249.65.32	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	15
66.249.65.43	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	15
66.249.65.14	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	14
66.249.65.48	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	13
66.249.65.1	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	13
66.249.65.48	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	12
66.249.65.36	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	12
66.249.65.12	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ip_Web_In	drop	12
66.249.65.191	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	11
66.249.78.173	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	11
66.249.65.50	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	11
66.249.65.5	United States	147.237.77.176	matpash.idf.il	Block_Ip_Web_In	drop	11
66.249.65.34	United States	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	11
66.249.65.72	United States	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	9
66.249.65.46	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	9
66.249.65.195	United States	147.237.0.34	tikshuv.idf.il	Block_Ip_Web_In	drop	9
66.249.73.209	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	8
66.249.67.115	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	8
66.249.79.69	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ip_Web_In	drop	7
66.249.93.164	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	7
66.249.73.230	United States	147.237.72.156	aman.idf.il	Block_Ip_Web_In	drop	7
66.249.73.231	United States	147.237.77.234	halag.idf.il	Block_Ip_Web_In	drop	6
66.249.65.37	United States	147.237.76.86	navy.idf.il	Block_Ip_Web_In	drop	6
66.249.67.107	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	6
66.249.84.182	United States	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	6
66.249.65.182	United States	147.237.77.74	law.idf.il	Block_Ip_Web_In	drop	6
66.249.65.41	United States	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	6
66.249.67.99	United States	147.237.76.30	himush.idf.il	Block_Ip_Web_In	drop	6

04-14-2015-05:03:08 to 04-14-2015-06:03:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	86
46.137.134.188	Ireland	147.237.72.156	aman.idf.il	DVRep_P-N_40-59	Permit	10
46.137.134.188	Ireland	147.237.72.166	aka.idf.il	DVRep_P-N_40-59	Permit	10
198.20.69.98	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.76.148	gqcenter.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.46	e.chinuch.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
162.244.81.173		147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
71.6.167.142	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
68.187.73.48	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
198.20.69.98	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.42	refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.44	e.refuah.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.19	law-forum.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
186.57.133.131	Argentina	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.8.28	e.mobile-ks.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1

04-14-2015-05:03:08 to 04-14-2015-06:03:08

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
82.80.25.221	Israel	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	8
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
80.55.55.59	Poland	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.76.202	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
213.136.84.245	Germany	147.237.77.216	dover.idf.il	ET SCAN NMAP -sS window 1024	1
59.41.39.125	China	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
176.104.213.250	Russian Federation	147.237.76.31	nakchal.idf.il	ET SCAN Potential SSH Scan	1
54.86.86.50	United States	147.237.77.216	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
122.228.207.76	China	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
91.217.90.19	Ukraine	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
80.55.55.59	Poland	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
80.55.55.59	Poland	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
59.41.39.125	China	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
59.41.39.125	China	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
122.228.207.76	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
5.196.147.122	Germany	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.72.166	aka.idf.il	ET SCAN Potential SSH Scan	1
104.197.30.168		147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 3072	1

04-14-2015-05:03:08 to 04-14-2015-06:03:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
203.117.143.129	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	72
69.65.89.121	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	65
27.123.169.166	Fiji	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	59
212.179.61.120	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	48
99.238.32.134	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	37
85.250.135.85	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
46.19.86.64	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	36
217.69.132.162	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	33
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	27
149.78.231.110	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	19
185.24.76.42	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	10
207.46.13.89	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
188.161.183.52	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	9
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
17.142.152.72	United States	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	8
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
93.172.34.126	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
135.23.80.19	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
17.142.152.111	United States	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	6
70.83.33.29	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
106.73.78.160	Japan	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
173.56.61.112	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
46.19.86.28	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
189.40.66.71	Brazil	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
207.46.13.82	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
184.74.244.201	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
17.142.152.81	United States	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	4
92.242.35.54	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
80.246.133.239	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	3
64.231.159.80	Canada	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
69.123.198.44	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
80.246.133.239	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
128.242.249.11	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
157.55.39.6	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
2.54.173.34	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.39.5.36	Russian Federation	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
17.142.152.86	United States	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	2
185.13.195.153	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.42	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
213.8.2.49	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
197.163.48.192	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.153	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
46.19.85.158	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
213.57.254.163	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
17.142.145.3	United States	147.237.77.176	matpash.idf.il	First packet isn't SYN	drop	drop	2

04-14-2015-05:03:08 to 04-14-2015-06:03:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
68.180.228.117	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.117	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
207.46.13.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/0505-4.stm	Block	1
95.173.189.7	Turkey	147.237.77.74	law.idf.il	Distributed Illegal HTTP Version	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/march/13.stm	Block	1
180.76.4.198	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
52.1.90.117	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
112.118.65.11	Hong Kong	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
23.20.28.24	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
180.76.5.75	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
157.55.39.41	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/defense.stm	Block	1
46.39.5.36	Russian Federation	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
184.105.139.67	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
157.55.39.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/iaf/present2.stm	Block	1
46.161.41.199	Russian Federation	147.237.72.166	aka.idf.il	Abnormally Long Request request version	Block	1
202.46.61.59	China	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il//modiin/default.aspx	Block	1
84.94.85.74	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mainqsachar	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.255.253.124	Block	1
178.162.205.80	Germany	147.237.77.19	law-forum.idf.il	Illegal HTTP Version	Block	1
46.161.41.199	Russian Federation	147.237.72.166	aka.idf.il	Illegal HTTP Version Ã®Ã²Ã¥Ã¸Ã¡Ã©Ã-, Ã¸Ã· Ã«Ã¹Ã©Ã·Ã¡Ã¸Ã¥ Ã Ã¥Ã°Ã- Ã¡Ã Ã¸Ã µ Ã©Ã¤Ã©Ã¤ Ã¬Ã¦Ã¤ Ã±Ã¥Ã³ Ã®Ã¥Ã§Ã¬Ã¨%22 HTTP/1.1	Block	1

04-14-2015-05:03:08 to 04-14-2015-06:03:08