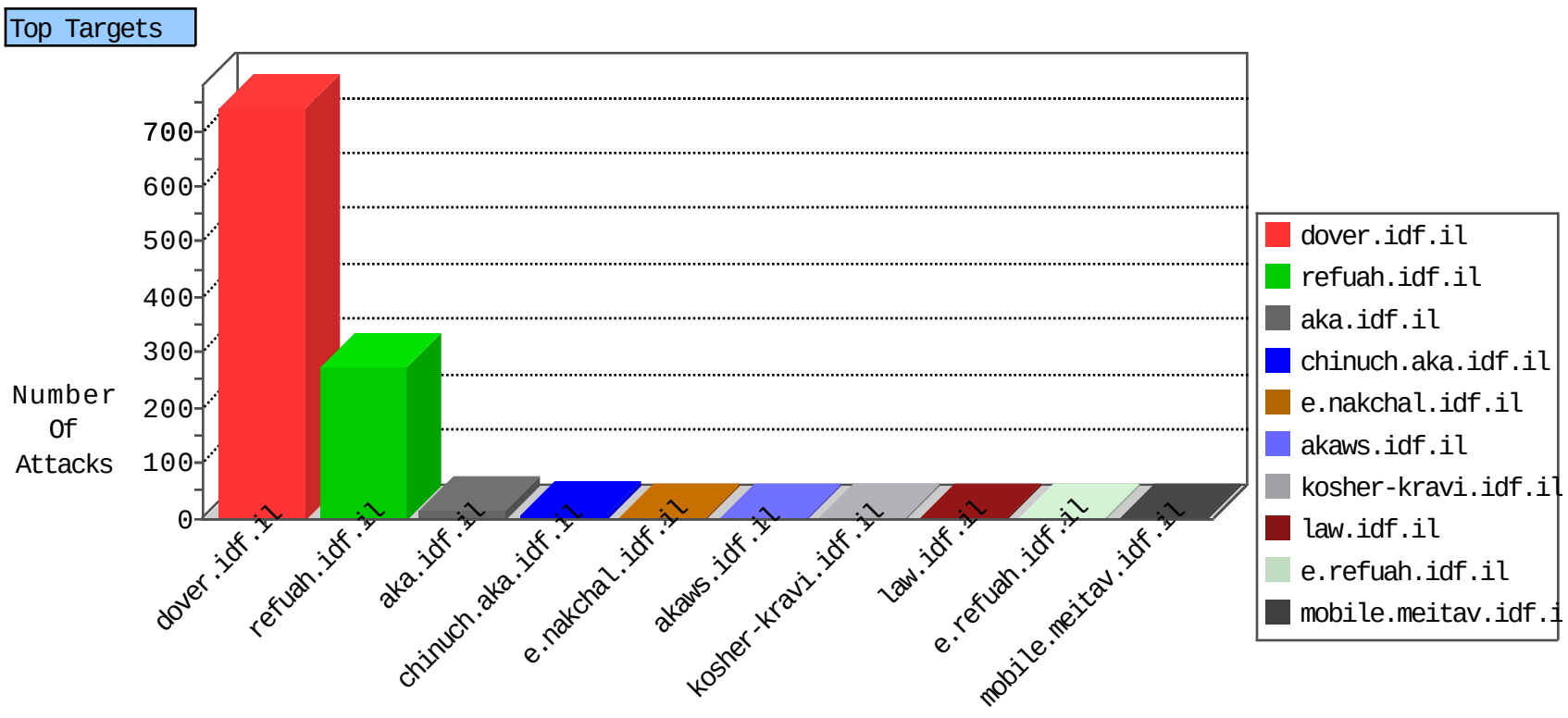
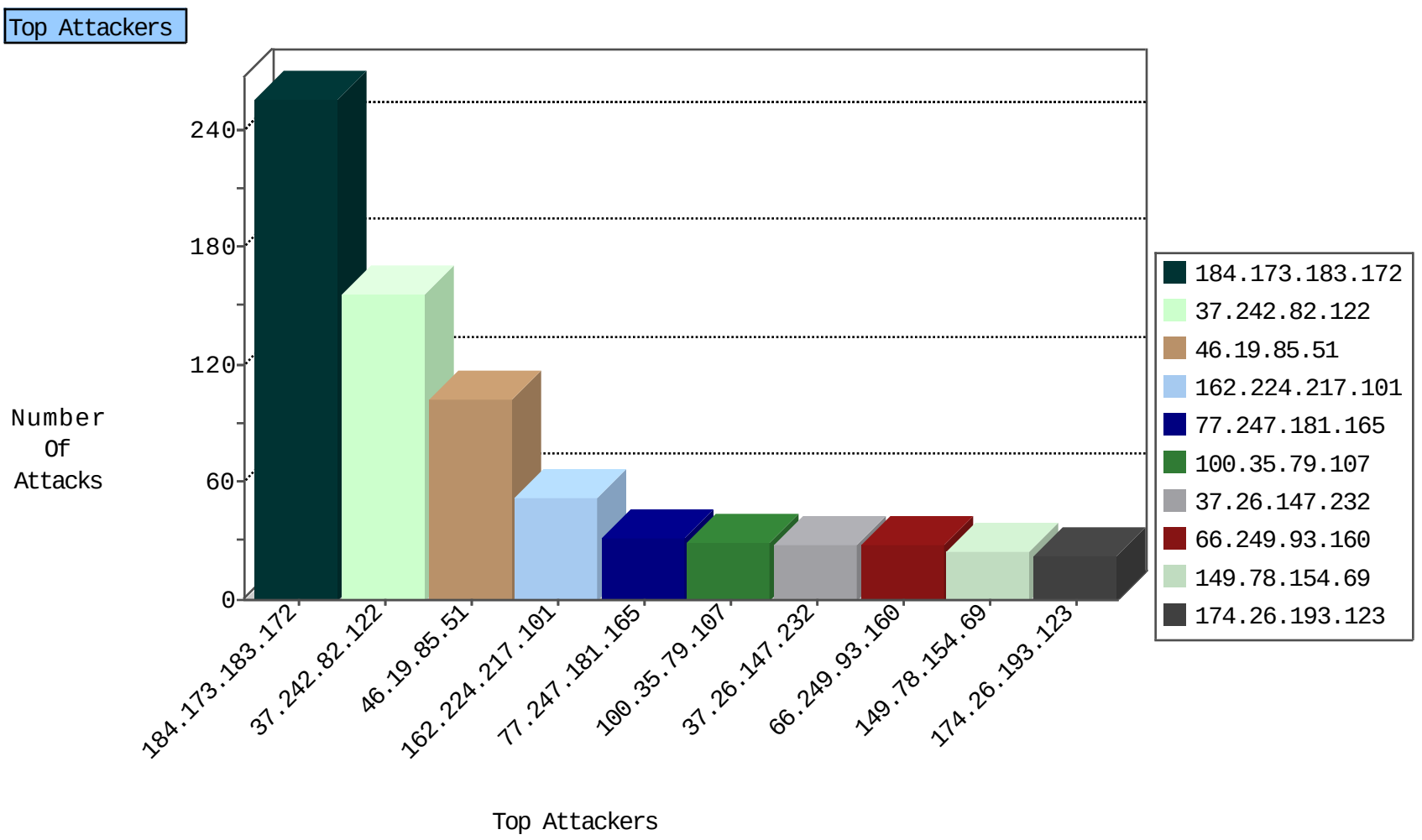
05-07-2015-03:03:05 to 05-07-2015-04:03:05

IDF Under Attack
05-07-2015-03:03:05





05-07-2015-03:03:05 to 05-07-2015-04:03:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.155	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	828
66.249.78.159	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	211
119.246.114.209	Hong Kong	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	2
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
100.35.79.107	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
72.174.199.213	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
195.37.190.86	Germany	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1

05-07-2015-03:03:05 to 05-07-2015-04:03:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.76.42	refuah.idf.il	DVRep_P-N_40-59	Permit	256
188.138.9.50	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	2
198.20.70.114	United States	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	2
188.138.9.50	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.72.167	ishurim.aka.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.72.156	aman.idf.il	DVRep_B-N_60_100	Block	1
46.19.86.231	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
198.20.69.98	United States	147.237.76.197	e.himush.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.233	atal.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.8.14	e.orchot.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
198.20.69.98	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
201.93.2.109	Brazil	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
188.138.9.50	Germany	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.212	e.dover.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.76.147	chinuch.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
198.20.70.114	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
188.138.9.50	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1

05-07-2015-03:03:05 to 05-07-2015-04:03:05

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
212.86.219.134	Germany	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	2
221.235.189.245	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
121.46.0.125	China	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 4096	1
221.235.189.245	China	147.237.72.14	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
80.82.78.27	Netherlands	147.237.0.15	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.189.245	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.76.177	ncore.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
221.235.189.245	China	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.76.200	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.230.71	United States	147.237.76.197	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.77.212	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
196.47.173.21	Cote D'Ivoire	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 2048	1
61.240.144.64	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
221.235.189.245	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
196.47.173.21	Cote D'Ivoire	147.237.77.74	law.idf.il	ET SCAN NMAP -f -sS	1
12.139.34.20	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 4096	1
221.235.189.245	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
188.138.9.51	Germany	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
221.235.189.245	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
175.136.197.37	Malaysia	147.237.76.147	chinuch.aka.idf.il	ET SCAN NMAP -sS window 3072	1
221.235.189.245	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
94.23.210.101	France	147.237.76.42	refuah.idf.il	SERVER-WEBAPP admin.php access	1
221.235.189.245	China	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.77.235	sviva.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
221.235.189.245	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.0.33	idf.il	ET SCAN Potential VNC Scan 5800-5820	1
61.240.144.65	China	147.237.76.198	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.230.71	United States	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
196.47.173.21	Cote D'Ivoire	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	China	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
221.235.189.245	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
12.139.34.20	United States	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
221.235.189.245	China	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
188.138.9.51	Germany	147.237.8.46	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1

05-07-2015-03:03:05 to 05-07-2015-04:03:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
37.242.82.122	Saudi Arabia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	156
46.19.85.51	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	102
162.224.217.101	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	52
77.247.181.165	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	29
37.26.147.232	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
66.249.93.160	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
100.35.79.107	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	28
149.78.154.69	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
174.26.193.123	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	22
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	18
66.249.93.164	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	15
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	14
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	12
212.199.182.150	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
172.4.49.43	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
220.255.1.117	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
188.165.15.99	France	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
70.39.187.201	Satellite Provider	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
201.209.191.117	Venezuela	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
66.249.64.238	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
213.57.114.180	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
5.228.42.20	Russian Federation	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	4
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
75.1.196.34	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
128.242.249.13	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
157.55.39.191	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
66.189.84.52	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
220.255.1.123	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
41.33.232.65	Egypt	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
2.54.40.136	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
72.93.169.190	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.78.173	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
157.55.39.67	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
65.19.138.34	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
98.167.45.57	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
220.255.1.156	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
79.176.119.61	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
37.142.216.100	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
72.174.199.213	United States	147.237.76.34	yohalan.idf.i		drop	drop	2
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
157.55.39.136	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
220.255.1.146	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
65.55.210.117	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
66.249.93.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2

05-07-2015-03:03:05 to 05-07-2015-04:03:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	7
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	4
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
41.105.125.234	Algeria	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 41.105.125.234	Block	2
99.4.122.139	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	2
41.105.125.234	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/undefined	Block	2
94.23.210.101	France	147.237.76.42	refuah.idf.il	PHP Attempt	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
87.253.145.16	Netherlands	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
66.249.75.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
207.46.13.26	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.67.134	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/m/	Block	1
157.55.39.135	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/organization/navy/dabur.stm	Block	1
94.23.210.101	France	147.237.76.42	refuah.idf.il	Admin Blocking	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1570-en/dover.aspx	Block	1
216.70.113.32	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
103.15.132.132	Hong Kong	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
68.180.229.51	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2002/march/14.stm	Block	1
66.249.67.194	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1267-he/refuah.aspx	Block	1
157.55.39.136	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/chamatz/klali/default.asp	None	1
94.23.210.101	France	147.237.76.42	refuah.idf.il	Multiple Admin Blocking from 94.23.210.101	Block	1
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1414-10832-he/dover.aspx	Block	1
66.249.64.151	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/contactus/contactus.aspx	Block	1
217.115.10.132	Germany	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
108.175.166.11	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
72.174.199.213	United States	147.237.76.30	himush.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
66.249.67.218	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1312-he/refuah.aspx	Block	1
188.165.15.99	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.99	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1485-12563-he/dover.aspx	Block	1
157.55.39.6	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
72.174.199.213	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to /tmunblock.cgi	Block	1
66.249.69.15	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/	Block	1
188.165.15.99	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/mrdr.stm	Block	1
94.23.210.101	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/administrator/	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-16576-ar/dover.aspxsee	Block	1

05-07-2015-03:03:05 to 05-07-2015-04:03:05