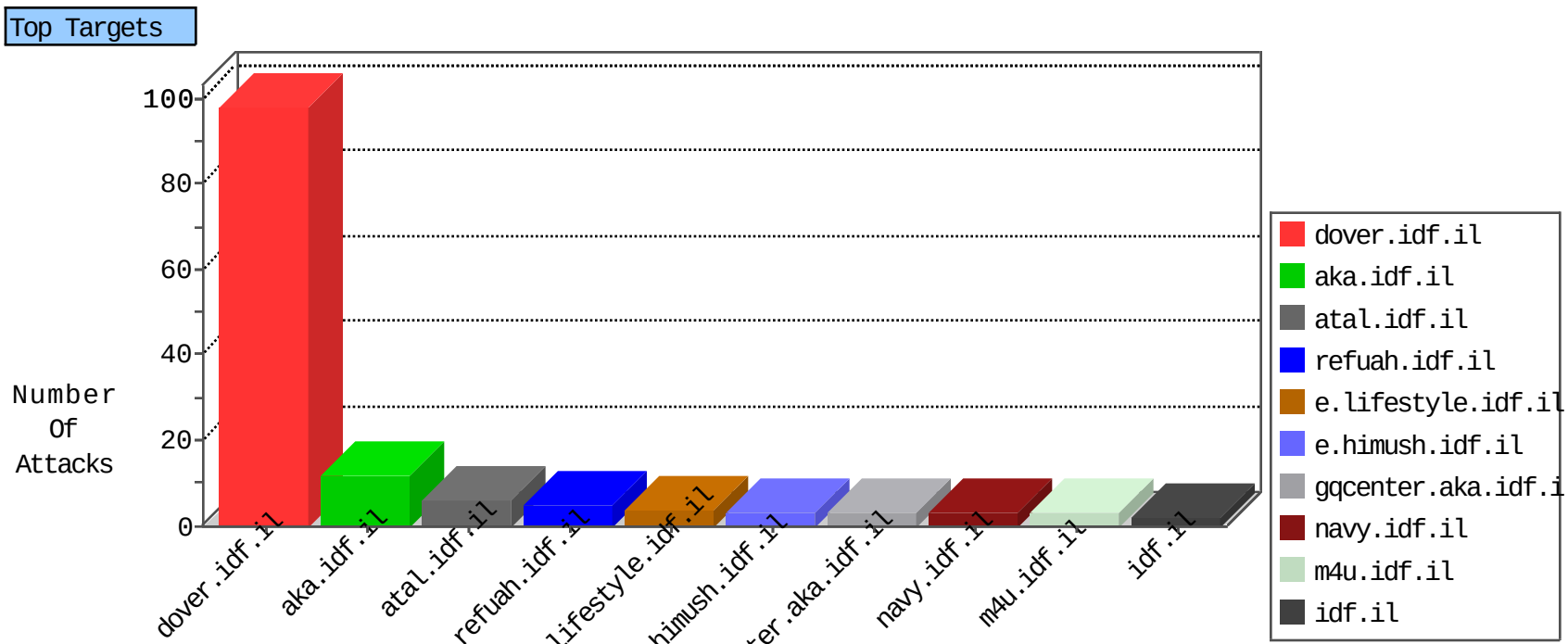
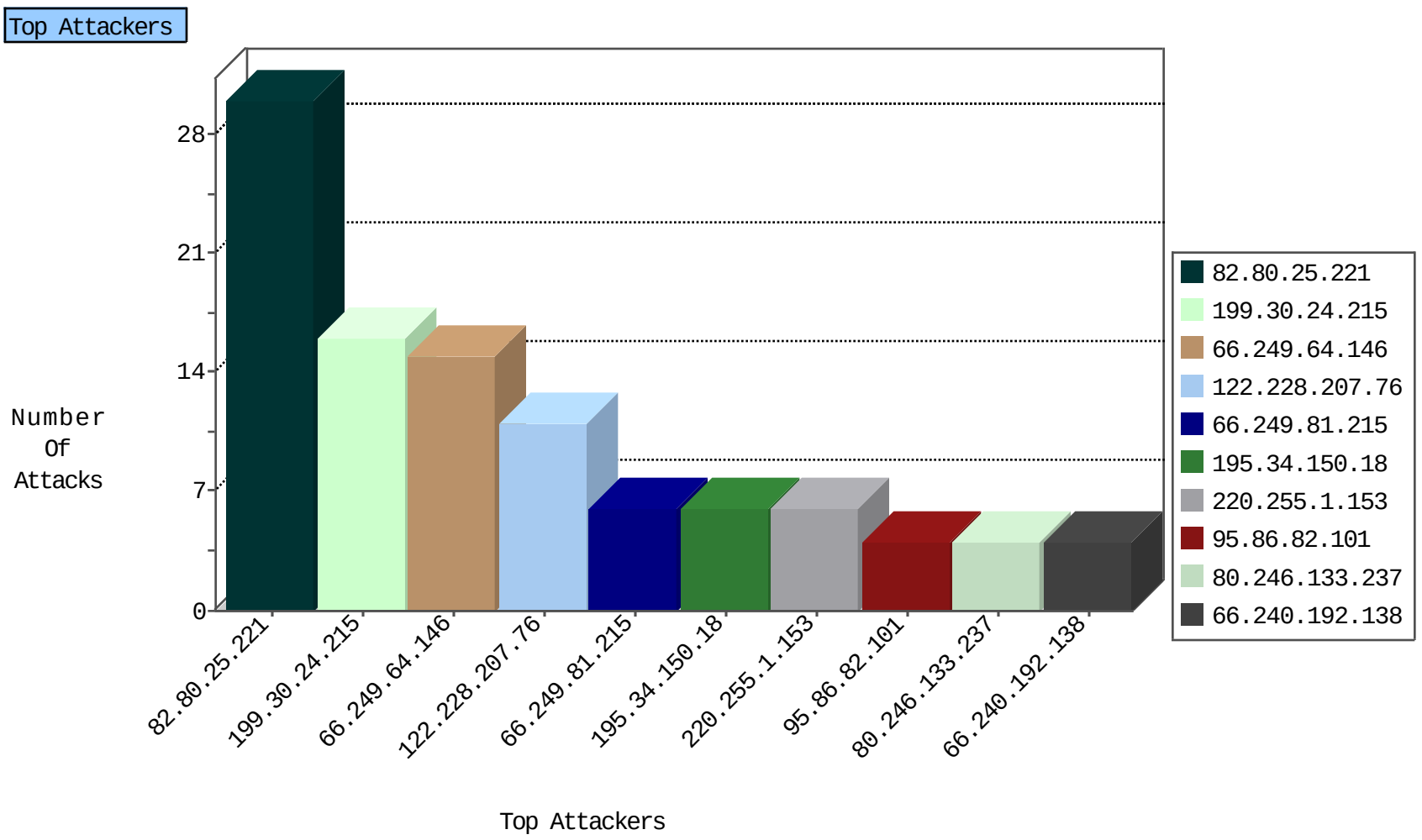
04-01-2015-03:03:06 to 04-01-2015-04:03:06

IDF Under Attack
04-01-2015-03:03:06

Top Targets



Top Attackers



04-01-2015-03:03:06 to 04-01-2015-04:03:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
124.232.142.220	China	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1

04-01-2015-03:03:06 to 04-01-2015-04:03:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
165.112.165.207	United States	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3
125.168.9.74	Australia	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
71.6.165.200	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
81.17.27.234	Switzerland	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.15	kosher-kravi.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	147.237.76.148	gqcenter.aka.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
85.25.103.50	Germany	147.237.76.177	ncore.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
71.6.167.142	United States	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.77.74	law.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.77.234	halag.idf.il	DVRep_B-N_60_100	Block	1
81.17.27.234	Switzerland	147.237.8.24	e.lifestyle.idf.il	DVRep_B-N_60_100	Block	1

04-01-2015-03:03:06 to 04-01-2015-04:03:06

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	30
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
178.19.107.114	Poland	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
114.255.149.210	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
128.61.240.66	United States	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
91.121.10.32	France	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	1
128.61.240.66	United States	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.77.234	halag.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.8.24	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
27.50.132.61	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 2048	1
122.228.207.76	China	147.237.77.121	e.navy.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
114.255.149.210	China	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
178.19.107.114	Poland	147.237.76.30	himush.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.132.118	Russian Federation	147.237.72.14	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
128.61.240.66	United States	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
122.228.207.76	China	147.237.77.233	atal.idf.il	ET SCAN Potential SSH Scan	1
27.217.226.249	China	147.237.0.33	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
122.228.207.76	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
27.50.132.61	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -f -sS	1
122.228.207.76	China	147.237.77.74	law.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
122.228.207.76	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1

04-01-2015-03:03:06 to 04-01-2015-04:03:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
199.30.24.215	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	16
66.249.64.146	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
66.249.81.215	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
220.255.1.153	Singapore	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
207.46.13.5	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
80.246.133.237	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	2
207.46.13.112	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
80.246.133.237	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	alert	2
141.212.122.67	United States	147.237.76.198	e.yohalan.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.85.131	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
184.105.247.236	United States	147.237.76.196	e.sviva.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
141.212.122.69	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
188.138.17.205	France	147.237.76.44	e.refuah.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
89.216.115.6		147.237.77.216	dover.idf.il	SAM rule	drop	drop	1
5.144.131.170	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
207.164.152.162	Canada	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
141.212.122.73	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	1
141.212.122.47	United States	147.237.76.148	gqcenter.aka.idf.i		drop	drop	1
38.111.147.86	United States	147.237.77.216	dover.idf.il		drop	drop	1
146.185.239.104	Russian Federation	147.237.8.24	e.lifestyle.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
74.82.47.14	United States	147.237.76.148	gqcenter.aka.idf.i		drop	drop	1
141.212.122.60	United States	147.237.0.200	m4u.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
38.229.1.15	United States	147.237.76.197	e.himush.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
146.185.239.104	Russian Federation	147.237.76.200	eitan.aka.idf.il		drop	drop	1

04-01-2015-03:03:06 to 04-01-2015-04:03:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
95.86.82.101	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	4
66.249.64.146	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.146	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
207.46.13.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/aaron.stm	Block	1
91.121.10.32	France	147.237.77.216	dover.idf.il	Multiple signatures from 91.121.10.32	Block	1
176.12.137.251	Israel	147.237.76.39	mobile.meitav.idf.i	Cookie Tampering on cookie .ASPNETAUTH: Expected 0102C4655895283AD208FEC4DD99602B3AD208000933003300360035003000310037003900360000012F00FF, Observed 0102CAC46373E439D208FECA3CA53EE739D208000933003300360035003000310037003900360000012F00FF	None	1
70.195.71.101	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
37.26.147.174	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __EVENTARGUMENT in www.aka.idf.il/main/sachar/	None	1
91.121.10.32	France	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.64.146	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/insignia/hogr.stm	Block	1
180.76.4.104	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
37.26.147.174	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
93.173.236.141	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
66.249.64.150	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/insignia/drgt.stm	Block	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
73.142.74.50	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.64.52	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.78.4	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
203.133.169.208	Korea, Republic of	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 203.133.169.208	Block	1
79.183.140.43	Israel	147.237.72.166	aka.idf.il	Unknown Parameter q in www.aka.idf.il/main/giyus/login.aspx	None	1
66.249.64.142	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/fatah/english/main_index.stm	Block	1
108.165.33.22	United States	147.237.72.156	aman.idf.il	Unauthorized Method HEAD for 147.237.72.156/	Block	1
68.180.228.50	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1

04-01-2015-03:03:06 to 04-01-2015-04:03:06