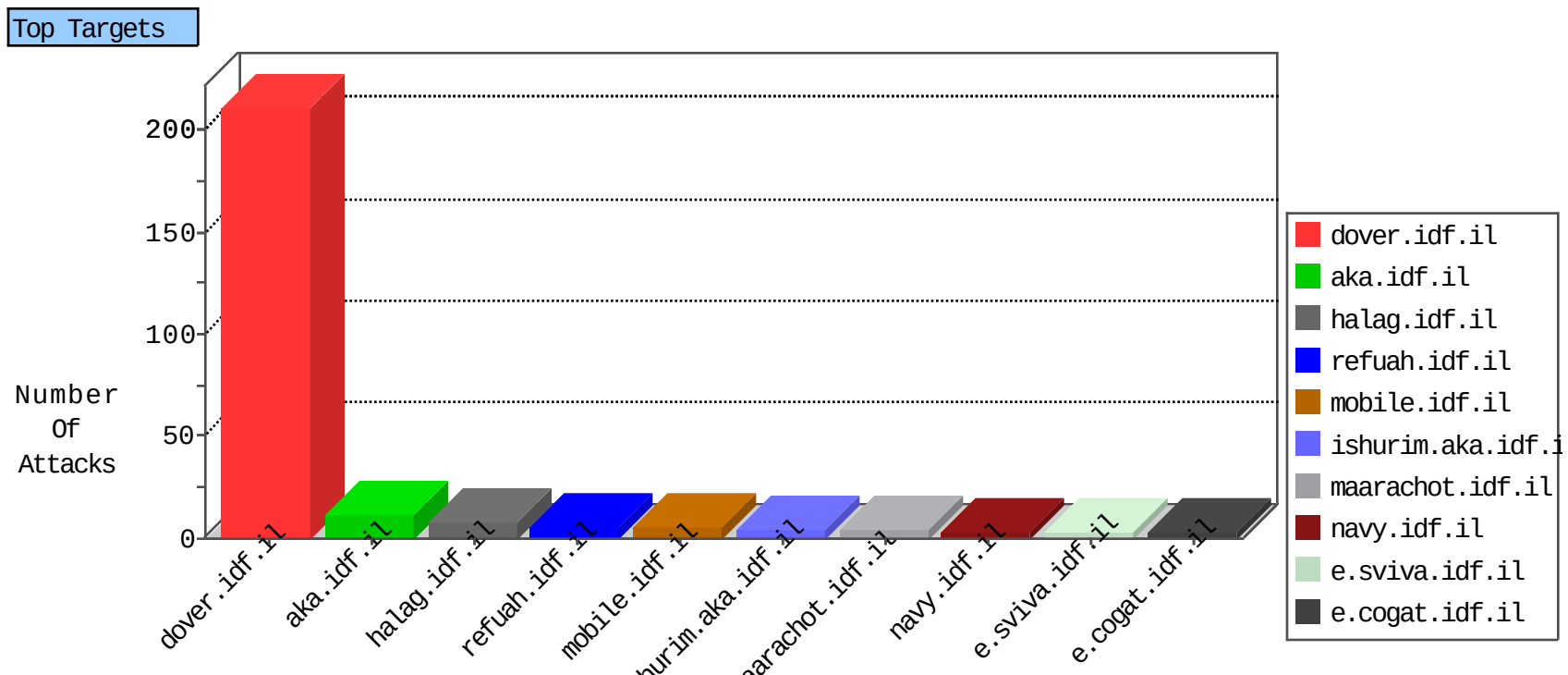
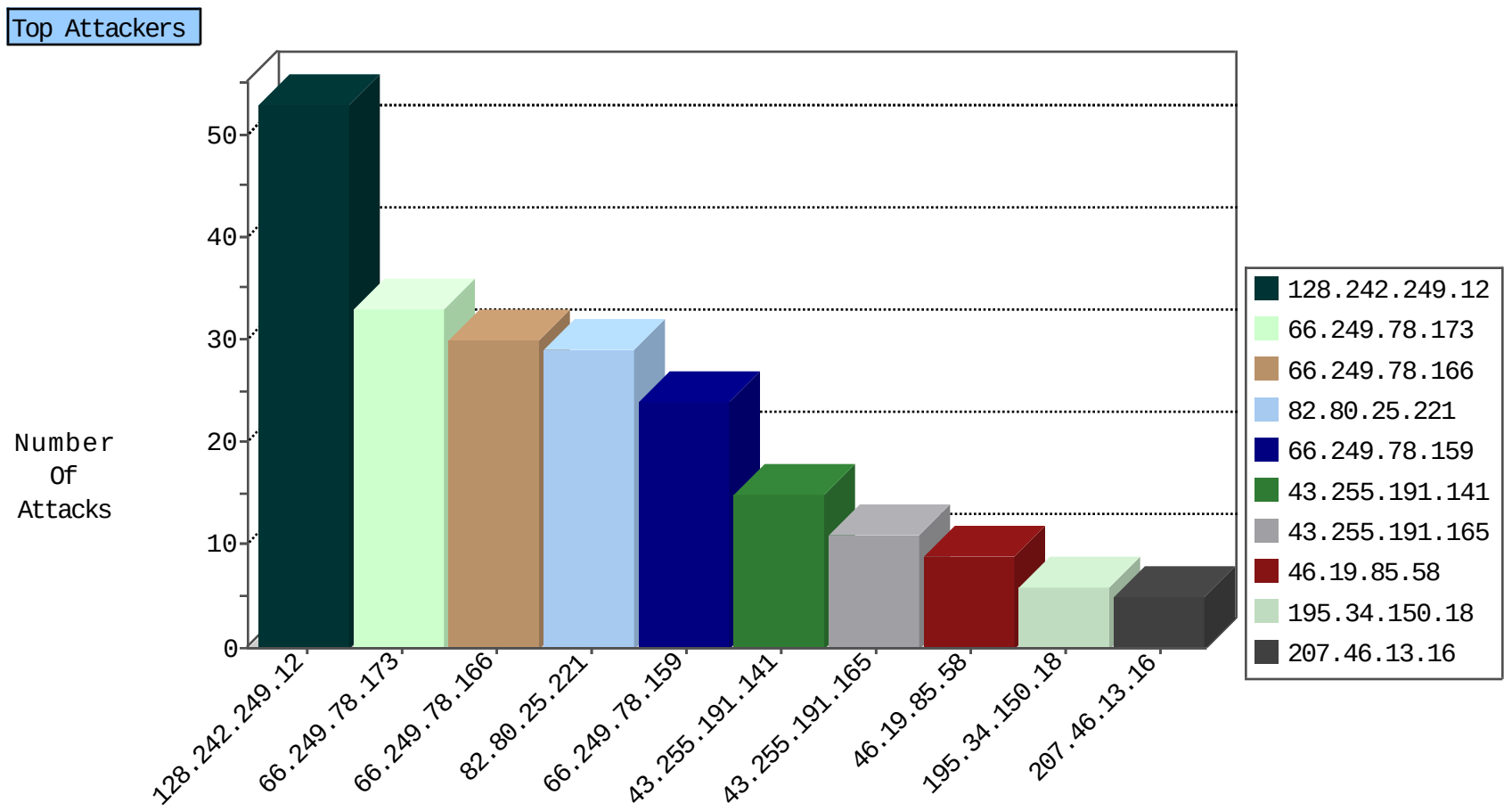
03-29-2015-03:03:01 to 03-29-2015-04:03:01

IDF Under Attack
03-29-2015-03:03:01

Top Targets



Top Attackers



03-29-2015-03:03:01 to 03-29-2015-04:03:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count

03-29-2015-03:03:01 to 03-29-2015-04:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
128.242.249.12	United States	147.237.77.216	dover.idf.il	DVRep_P-N_40-59	Permit	53
24.95.94.194	United States	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	4
212.76.115.250	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
77.127.132.2	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.250.146.221	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
104.232.3.33		147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
46.19.85.58	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1

03-29-2015-03:03:01 to 03-29-2015-04:03:01

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	29
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
43.255.191.165	Japan	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
183.136.216.7	China	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
131.104.106.84	Canada	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.141	Japan	147.237.77.170	maarachot.idf.il	ET SCAN Potential SSH Scan	1
220.226.22.210	India	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.76.197	e.himush.idf.il	ET SCAN Potential SSH Scan	1
220.226.22.210	India	147.237.0.16	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.77.243	mobile.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.76.176	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
212.147.56.190	Switzerland	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.165	Japan	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
212.147.56.190	Switzerland	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.141	Japan	147.237.76.39	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.77.205	prisha.idf.il	ET SCAN Potential SSH Scan	1
187.58.224.213	Brazil	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.141	Japan	147.237.72.167	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
187.58.224.213	Brazil	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.141	Japan	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.0.15	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
183.136.216.7	China	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
183.136.216.7	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.77.227	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
220.226.22.210	India	147.237.0.34	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
131.104.106.84	Canada	147.237.77.170	maarachot.idf.il	ET SCAN NMAP -f -sS	1
43.255.191.141	Japan	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
220.226.22.210	India	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.141	Japan	147.237.76.177	ncore.idf.il	ET SCAN Potential SSH Scan	1
218.77.79.43	China	147.237.72.217	e.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
43.255.191.165	Japan	147.237.77.235	sviva.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
212.147.56.190	Switzerland	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
43.255.191.165	Japan	147.237.77.216	dover.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.76.34	yohalan.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.77.179	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
187.58.224.213	Brazil	147.237.77.61	e.cogat.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.141	Japan	147.237.72.156	aman.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.165	Japan	147.237.76.200	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
183.136.216.7	China	147.237.76.202	e.halag.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.141	Japan	147.237.8.28	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1

03-29-2015-03:03:01 to 03-29-2015-04:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	30
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	24
46.19.85.58	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	7
66.249.75.66	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
46.19.85.118	Israel	147.237.77.243	mobile.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
31.186.228.88	United Kingdom	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
31.186.228.92	United Kingdom	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
31.186.228.62	United Kingdom	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
190.236.154.189	Peru	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	2
31.186.228.66	United Kingdom	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
207.46.13.16	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
66.249.75.74	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
109.67.49.235	Israel	147.237.76.42	refuah.idf.il	First packet isn't SYN	drop	drop	1
46.19.85.129	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
208.64.28.130	United States	147.237.76.86	navy.idf.il	Failed to handle connection data	Block HTTP Non Compliant	monitor	1
141.212.122.177	United States	147.237.76.201	e.atal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.86.144	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
46.19.85.58	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
188.138.17.205	France	147.237.0.200	m4u.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
46.19.86.243	Israel	147.237.0.34	tikshuv.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
79.178.173.134	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.173	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	3
157.55.39.42	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.42	Block	3
85.130.226.9	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
207.46.13.16	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.16	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
46.117.94.164	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/rabanut/webresource.axd	Block	2
190.236.154.189	Peru	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/default.aspx en espaÃ±ol	Block	1
115.25.81.70	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
184.173.183.173	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/&usg=alkjrhgxiuhxu6qop_9m_mdye-iohr_2ia	Block	1
66.249.78.160	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/matash	Block	1
207.46.13.16	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
155.254.245.94		147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
188.138.17.205	France	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/	Block	1
157.55.39.41	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/0218-4.stm	Block	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
188.165.15.60	France	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/163-5486-he/patzar.aspx	Block	1
188.165.15.196	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.165.15.196	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.58	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/search.asp	Block	1