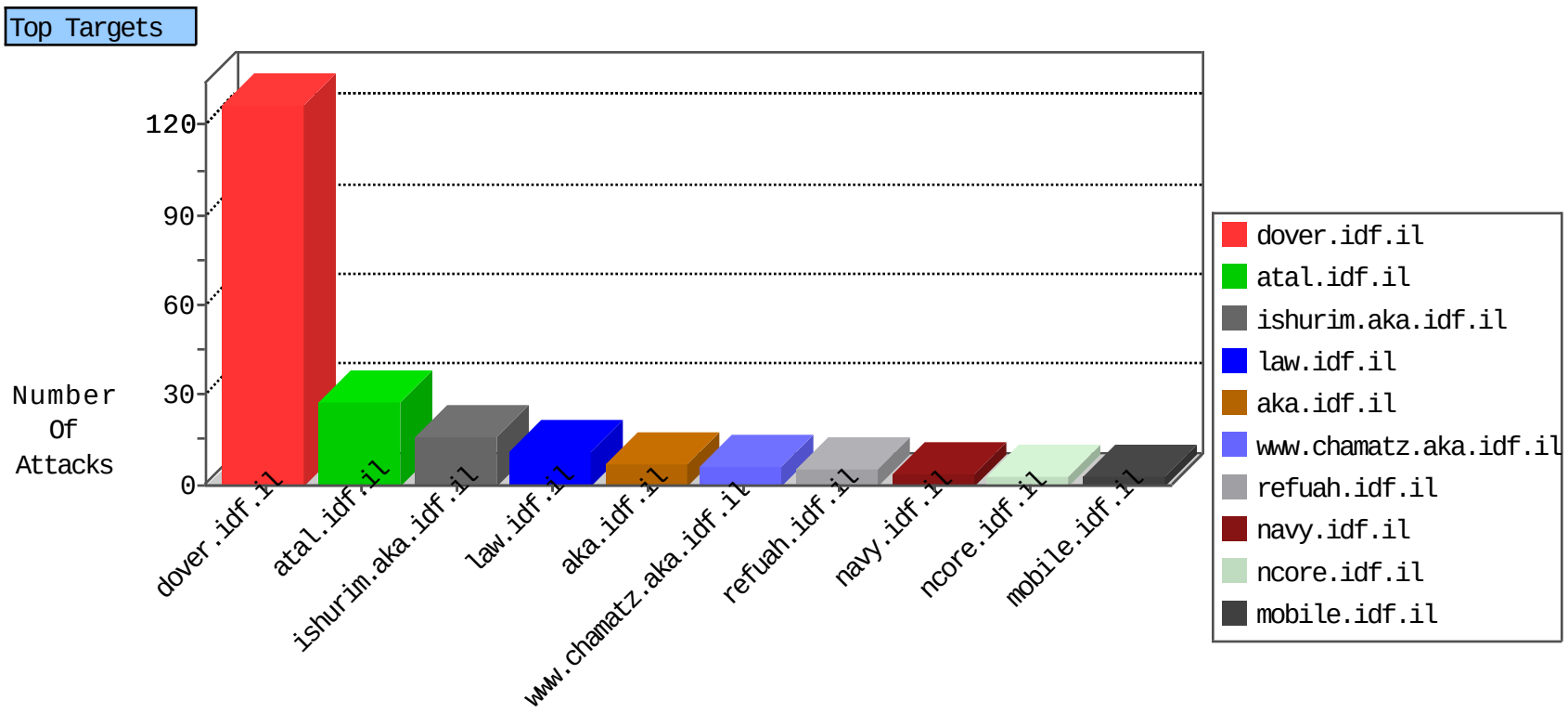
04-24-2015-03:03:03 to 04-24-2015-04:03:03

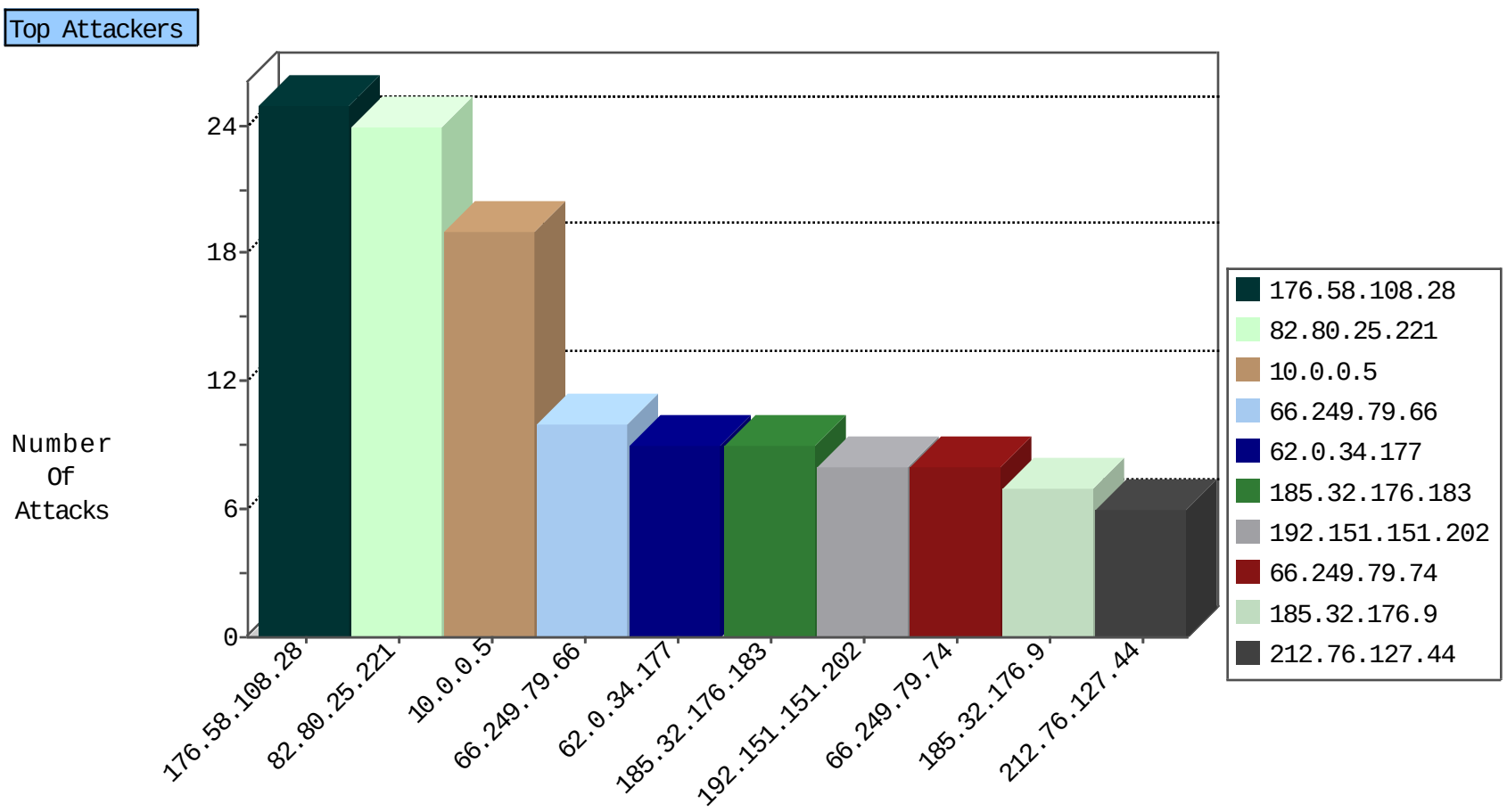
IDF Under Attack
04-24-2015-03:03:03

Top Targets



Top Target

Top Attackers



Top Attackers

04-24-2015-03:03:03 to 04-24-2015-04:03:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.92	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	971
185.32.176.9	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	81
185.32.176.183	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	81
66.249.78.166	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	36
10.0.0.5		147.237.77.233	atal.idf.il	Invalid TCP Flags	drop	19
62.0.34.177	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	9
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
141.138.156.16	France	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1

04-24-2015-03:03:03 to 04-24-2015-04:03:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
198.20.69.98	United States	147.237.77.226	www.chamatz.aka.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.227	e.hamaz.idf.il	DVRep_B-N_60_100	Block	1

04-24-2015-03:03:03 to 04-24-2015-04:03:03

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	24
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	5
66.249.65.34	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
91.224.132.118	Russian Federation	147.237.76.44	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.66	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
222.69.94.13	China	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 3072	1
61.16.232.231	India	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
198.20.69.74	United States	147.237.77.243	mobile.idf.il	ET DROP Dshield Block Listed Source	1
60.18.162.244	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 4096	1
193.107.16.206	Russian Federation	147.237.77.205	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
58.20.54.249	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
140.210.1.248	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 4096	1
140.210.1.248	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -f -sS	1
91.224.132.118	Russian Federation	147.237.76.177	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.132.118	Russian Federation	147.237.72.156	aman.idf.il	ET SCAN NMAP -sS window 1024	1
61.183.128.6	China	147.237.0.33	idf.il	ET SCAN NMAP -sS window 1024	1
201.239.118.143	Chile	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 4096	1
61.16.232.231	India	147.237.76.38	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
60.18.162.244	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
193.107.16.206	Russian Federation	147.237.77.205	prisha.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
140.210.1.248	China	147.237.77.233	atal.idf.il	ET SCAN NMAP -sS window 2048	1
140.210.1.248	China	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 4096	1

04-24-2015-03:03:03 to 04-24-2015-04:03:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
176.58.108.28	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	25
212.76.127.111	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
212.76.127.44	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
199.30.24.236	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
212.76.127.212	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
68.180.228.117	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
184.173.183.173	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
108.54.214.201	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
220.181.108.176	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
82.80.51.141	Israel	147.237.77.233	atal.idf.il	SYN retransmit with different window scale	Bad TCP sequence	alert	1
198.48.92.104	United States	147.237.76.200	eitan.aka.idf.il		drop	drop	1
217.69.136.205	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
116.193.159.42	Hong Kong	147.237.77.178	e.matpash.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
203.127.96.219	Singapore	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
62.0.34.177	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1
220.181.108.150	China	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	1

04-24-2015-03:03:03 to 04-24-2015-04:03:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.79.66	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.66	Block	9
66.249.79.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.74	Block	8
192.151.151.202	United States	147.237.77.74	law.idf.il	Multiple Admin Blocking from 192.151.151.202	Block	7
66.249.79.58	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.79.58	Block	4
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
82.80.51.141	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.73.213	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//	Block	1
66.249.65.28	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/993/patzar.aspx	Block	1
188.165.15.222	France	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.65.157	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
157.55.39.4	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/resources/chinuch/styles/import/bottomnavigaton.asp	Block	1
66.249.73.229	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/938-he/hamaz.aspx	Block	1
66.249.65.41	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
192.151.151.202	United States	147.237.77.74	law.idf.il	Admin Blocking	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
66.249.65.178	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	1
2.54.13.216	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233//1134-he/atal.aspx	Block	1
185.61.138.244		147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.65.43	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
69.171.227.112	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.65.181	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
46.118.119.63	Ukraine	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
188.165.15.13	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0216-1.stm	Block	1
66.249.65.60	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/	Block	1
198.20.69.74	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
66.249.73.203	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/×œ×›×ª×‘×″ ×″×žœ×?×″	Block	1
66.249.65.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
188.165.15.94	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/iturim/asp/list.asp	Block	1
66.249.79.66	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.stm	Block	1
66.249.65.70	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/938-he/refuah.aspx	Block	1

04-24-2015-03:03:03 to 04-24-2015-04:03:03