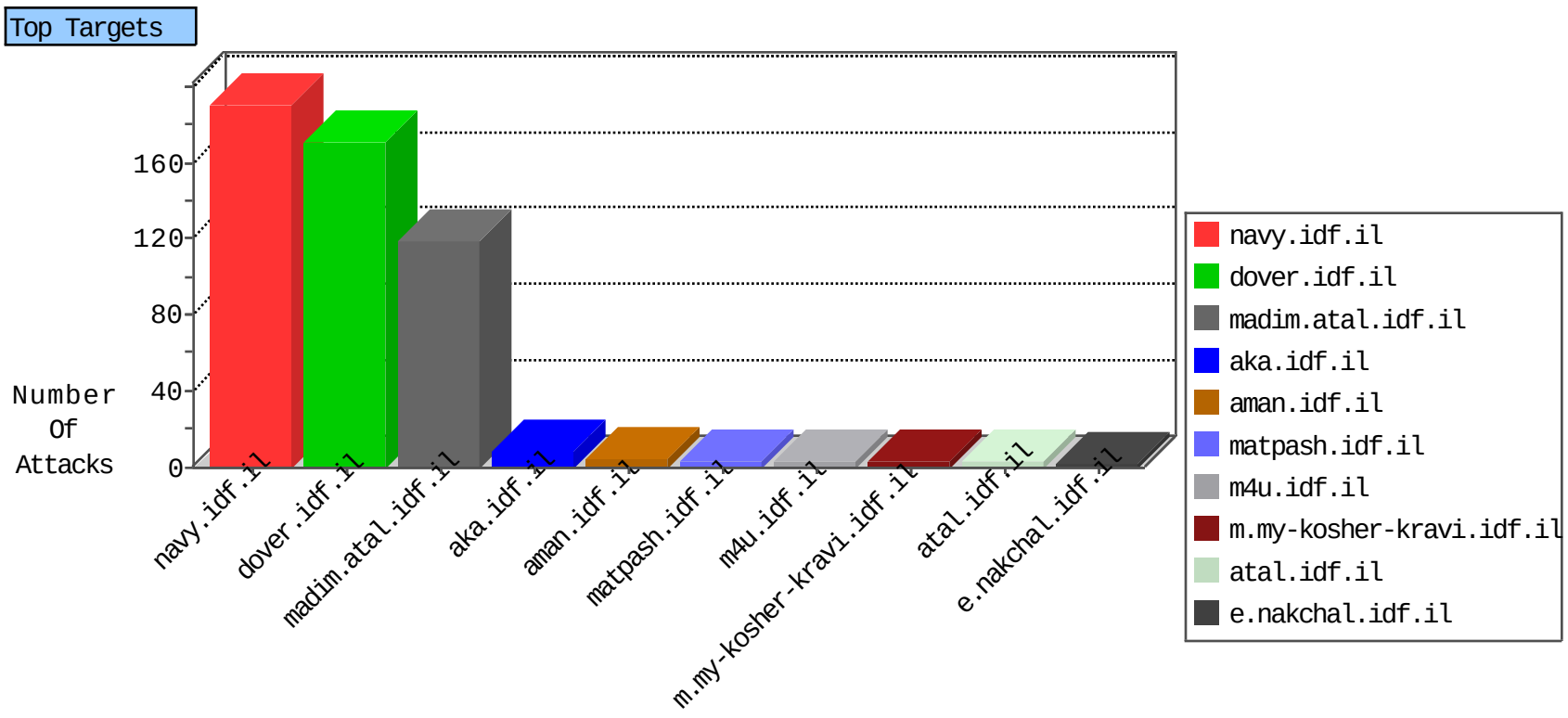
03-28-2015-04:03:01 to 03-28-2015-05:03:01

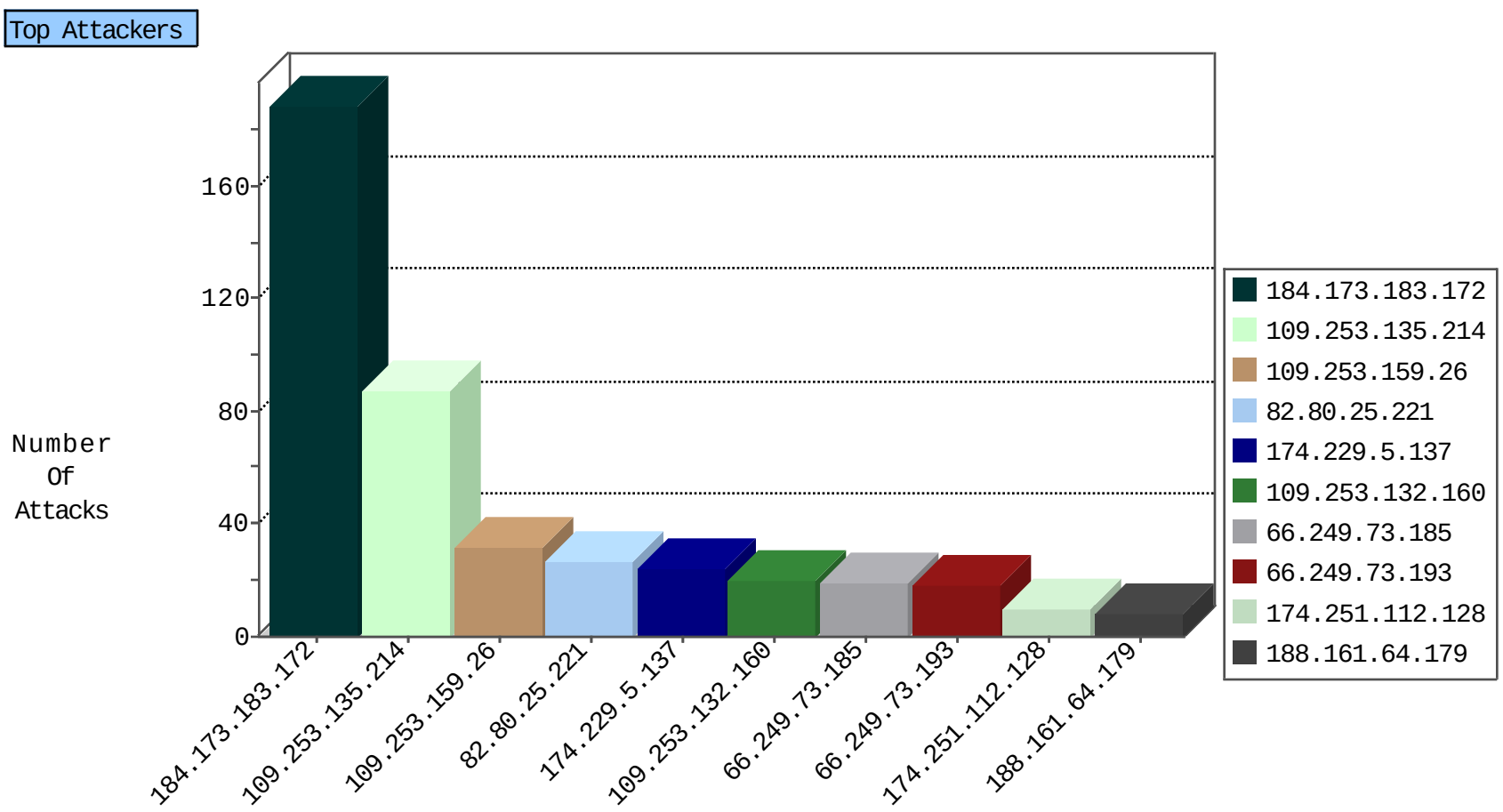
IDF Under Attack
03-28-2015-04:03:01

Top Targets



Top Target

Top Attackers



Top Attackers

03-28-2015-04:03:01 to 03-28-2015-05:03:01

Top Attackers In DDoS-Defence

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

03-28-2015-04:03:01 to 03-28-2015-05:03:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.76.86	navy.idf.il	DVRep_P-N_40-59	Permit	189
37.187.129.166	France	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	6
62.210.170.27	France	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	2
18.239.0.155	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	2
85.25.43.94	Germany	147.237.76.176	test.ncore.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.0.17	m.my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
185.14.28.27	Netherlands	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
77.127.132.2	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
162.220.56.186	United States	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
188.113.114.120	Norway	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.15	kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
176.10.99.204	Switzerland	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
188.161.64.179	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
85.25.43.94	Germany	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
178.62.219.113	Netherlands	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1

03-28-2015-04:03:01 to 03-28-2015-05:03:01

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	27
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
188.161.64.179	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	GPL WEB_SERVER /etc/passwd	1
94.102.50.56	Netherlands	147.237.77.234	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
58.20.54.249	China	147.237.72.167	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
188.161.64.179	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SQL Injection - Select From	1
182.74.17.72	India	147.237.72.166	aka.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.50.56	Netherlands	147.237.76.177	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.64	China	147.237.77.243	mobile.idf.il	ET SCAN NMAP -sS window 1024	1

03-28-2015-04:03:01 to 03-28-2015-05:03:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
109.253.132.160	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	20
66.249.73.193	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
66.249.73.185	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	18
174.229.5.137	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	8
174.229.5.137	United States	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	8
174.229.5.137	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	alert	8
174.251.112.128	United States	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
174.251.112.128	United States	147.237.77.216	dover.idf.il	Invalid sequence number	Bad TCP sequence	monitor	5
109.253.138.104	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
66.249.73.201	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	3
42.114.228.137	Vietnam	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
141.212.122.88	United States	147.237.0.200	m4u.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
95.130.15.96	France	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
109.253.138.127	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
89.207.133.55	Netherlands	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
18.239.0.140	United States	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
184.105.139.123	United States	147.237.76.196	e.sviva.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
141.212.122.183	United States	147.237.76.199	e.nakchal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
104.232.1.100		147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
116.193.159.52	Hong Kong	147.237.76.202	e.halag.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
91.121.104.168	France	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
37.187.51.210	France	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
212.179.102.163	Israel	147.237.72.156	aman.idf.il	First packet isn't SYN	drop	drop	1
141.212.122.184	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
70.39.187.108	Satellite Provider	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	1
141.212.122.84	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
91.213.8.236	Ukraine	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
142.4.213.25	Canada	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
85.24.215.117	Sweden	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
5.196.248.85	Germany	147.237.0.200	m4u.idf.il		drop	drop	1
141.212.122.87	United States	147.237.76.199	e.nakchal.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
94.159.143.166	Israel	147.237.77.170	maarachot.idf.il	Invalid ACK number	Bad TCP sequence	monitor	1
109.253.138.127	Israel	147.237.77.233	atal.idf.il	Invalid ACK number	Bad TCP sequence	alert	1
85.25.103.119	Germany	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
18.187.1.68	United States	147.237.77.216	dover.idf.il	directory traversal overflow	Directory Traversal	monitor	1
178.79.184.233	United Kingdom	147.237.0.200	m4u.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
109.253.135.214	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 109.253.135.214	Block	86
109.253.159.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	32
188.161.64.179	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.161.64.179	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
94.180.61.227	Russian Federation	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 94.180.61.227	Block	2
91.121.104.168	France	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
66.249.69.36	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//	Block	1
217.12.204.117	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
188.161.64.179	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/abc123/	Block	1
66.249.69.127	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il//modiin/default.aspx	Block	1
159.224.160.225	Ukraine	147.237.72.166	aka.idf.il	Unknown Parameter docId Result: ×?×• ×?×?×¨×›×ž ×¡Ã¼ ×¤×ž× ×œÃ» ×″×›Ã¿ ×ž×¢×Ÿ× ×?×′×š×˜; in www.aka.idf.il/brothers/skira/default.asp	None	1
84.109.177.100	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/default.aspx	None	1
188.165.15.121	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-8517-he/atal.aspx	Block	1
94.180.61.227	Russian Federation	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.73.185	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.185	Block	1
188.138.1.218	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Untraceable SSL Sessions from 188.138.1.218 (Unknown Server Certificate)	None	1
84.109.177.100	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
42.114.228.137	Vietnam	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
208.80.194.125	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166//	Block	1
109.253.135.214	Israel	147.237.0.19	madim.atal.idf.il	Too Many 404: Response Code per Session	Block	1
66.249.75.15	United States	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on list.ips.gov.il//modiin/default.aspx	Block	1
188.138.1.218	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unknown Server Certificate	None	1
84.109.177.100	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	1
66.249.69.15	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
216.211.108.224	Canada	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.75.117	United States	147.237.72.166	aka.idf.il	Unknown Parameter newsItem in www.aka.idf.il/megurim/news/	None	1