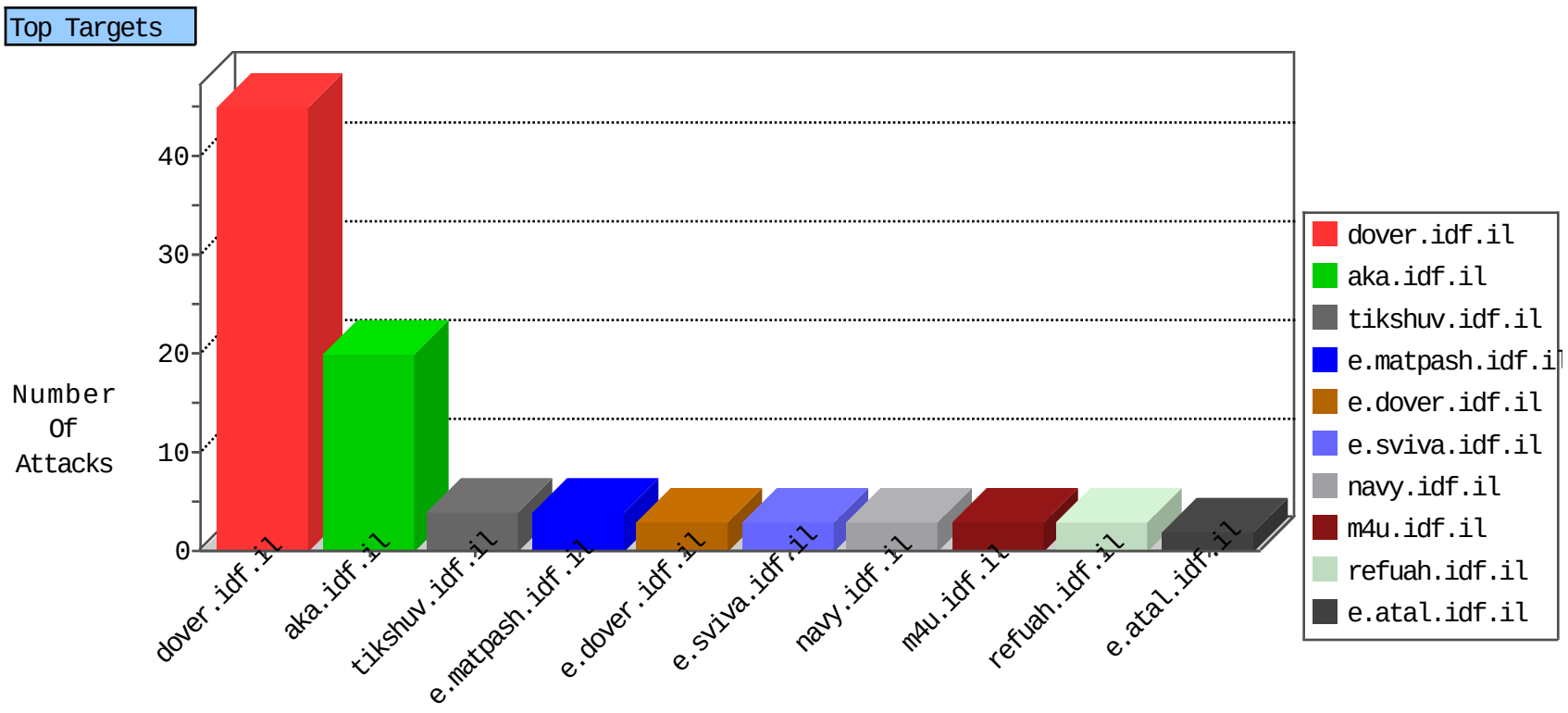
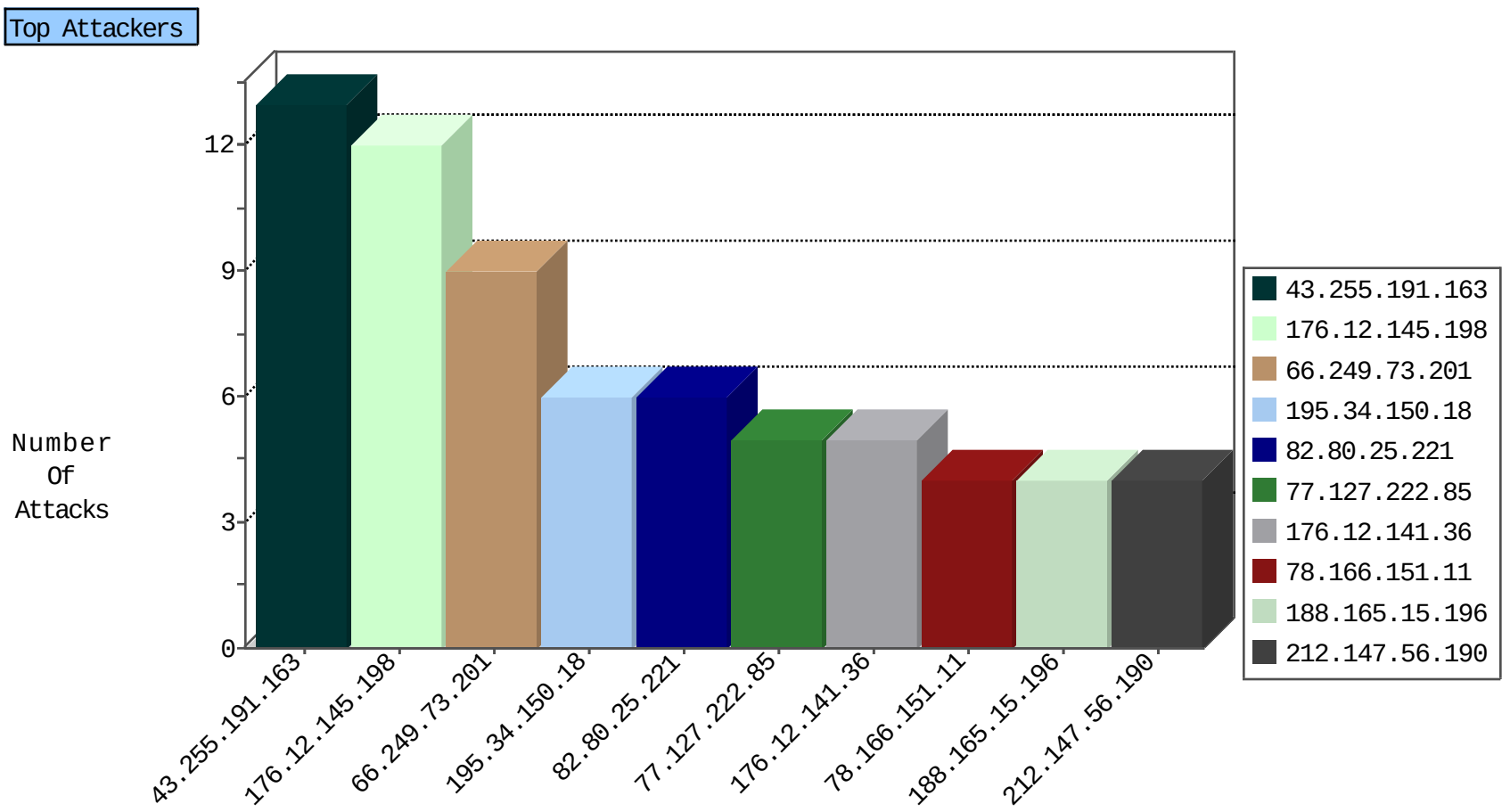
03-28-2015-07:03:02 to 03-28-2015-08:03:02

IDF Under Attack
03-28-2015-07:03:02

Top Targets



Top Attackers



03-28-2015-07:03:02 to 03-28-2015-08:03:02

Top Attackers In DDoS-Defence

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

03-28-2015-07:03:02 to 03-28-2015-08:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
77.127.132.2	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	2
85.25.43.94	Germany	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
85.250.189.52	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
78.166.151.11	Turkey	147.237.72.166	aka.idf.il	5056: HTTP: Cross Site Scripting (Javascript in HTTP request)	Permit	1
93.120.27.62	Romania	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
78.166.151.11	Turkey	147.237.72.166	aka.idf.il	C025: HTTP: access to administrator/index.php -> Quarantine	Block	1
93.120.27.62	Romania	147.237.72.14	dover.idf.il(old)	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.76.30	himush.idf.il	DVRep_B-N_60_100	Block	1
185.82.216.119		147.237.72.166	aka.idf.il	DVRep_B-N_60_100	Block	1

03-28-2015-07:03:02 to 03-28-2015-08:03:02

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	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
43.255.191.163	Japan	147.237.8.45	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
104.43.14.101		147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 2048	1
43.255.191.163	Japan	147.237.0.17	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
103.41.124.60		147.237.0.35	akaws.idf.il	ET SCAN Potential SSH Scan	1
216.189.148.175	United States	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 3072	1
78.166.151.11	Turkey	147.237.72.166	aka.idf.il	INDICATOR-OBFUSCATION script tag in POST parameters - likely cross-site scripting	1
212.147.56.190	Switzerland	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
43.255.191.163	Japan	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
212.147.56.190	Switzerland	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
43.255.191.163	Japan	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
187.9.27.231	Brazil	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.163	Japan	147.237.76.196	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
115.231.218.147	China	147.237.76.201	e.atal.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.76.86	navy.idf.il	ET SCAN Potential SSH Scan	1
115.231.218.147	China	147.237.76.30	himush.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.8.50	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
104.43.14.101		147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.163	Japan	147.237.0.33	idf.il	ET SCAN Potential SSH Scan	1
104.43.14.101		147.237.77.178	e.matpash.idf.il	ET SCAN NMAP -f -sS	1
216.189.148.175	United States	147.237.76.196	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
212.147.56.190	Switzerland	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.163	Japan	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
212.147.56.190	Switzerland	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.163	Japan	147.237.77.212	e.dover.idf.il	ET SCAN Potential SSH Scan	1
212.147.56.190	Switzerland	147.237.0.34	tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
43.255.191.163	Japan	147.237.77.19	law-forum.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.76.198	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
157.55.39.132	United States	147.237.0.34	tikshuv.idf.il	LOCAL_RULES DOS attack 01/2012	1
43.255.191.163	Japan	147.237.76.147	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
115.231.218.147	China	147.237.76.199	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
43.255.191.163	Japan	147.237.76.38	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
115.231.218.147	China	147.237.0.200	m4u.idf.il	ET SCAN Potential SSH Scan	1

03-28-2015-07:03:02 to 03-28-2015-08:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
176.12.145.198	Israel	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	12
66.249.73.201	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	8
176.12.141.36	Israel	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
77.127.222.85	Israel	147.237.72.166	aka.idf.il	First packet isn't SYN	drop	drop	4
188.165.15.196	France	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	2
96.52.141.48	Canada	147.237.0.200	m4u.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	2
188.138.17.205	France	147.237.77.227	e.hamaz.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
141.212.122.49	United States	147.237.76.197	e.himush.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
141.212.122.85	United States	147.237.76.197	e.himush.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
141.212.122.89	United States	147.237.72.217	e.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
188.138.1.218	Germany	147.237.77.227	e.hamaz.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
141.212.122.181	United States	147.237.77.61	e.cogat.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	1
188.138.17.205	France	147.237.76.200	eitan.aka.idf.i		drop	drop	1
141.212.122.46	United States	147.237.8.50	e.tikshuv.idf.i	Geo-location inbound enforcement	Geo-location enforcement	drop	1
141.212.122.196	United States	147.237.8.24	e.lifestyle.idf	Geo-location inbound enforcement	Geo-location enforcement	drop	1

03-28-2015-07:03:02 to 03-28-2015-08:03:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
46.121.64.113	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	3
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
176.12.141.36	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.73.201	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.73.201	Block	1
188.165.15.148	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/iturim/asp/list.asp	Block	1
78.166.151.11	Turkey	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
5.255.253.124	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/russian/main.stm	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.255.215.87	Block	1
66.249.73.228	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	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
79.176.34.189	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim/asp/6_s3_	Block	1
31.193.51.59	France	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18670-en/kkkkkkk=c37066e4kkkkkkk_c37066e4	Block	1
66.249.79.59	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
188.165.15.196	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/announcements/2001/april/8.stm	Block	1
149.78.230.248	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/rabanut/webresource.axd	Block	1
188.165.15.148	France	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
157.55.39.55	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
66.249.73.185	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
188.165.15.148	France	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	1
77.127.222.85	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEGENERATOR in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1

03-28-2015-07:03:02 to 03-28-2015-08:03:02