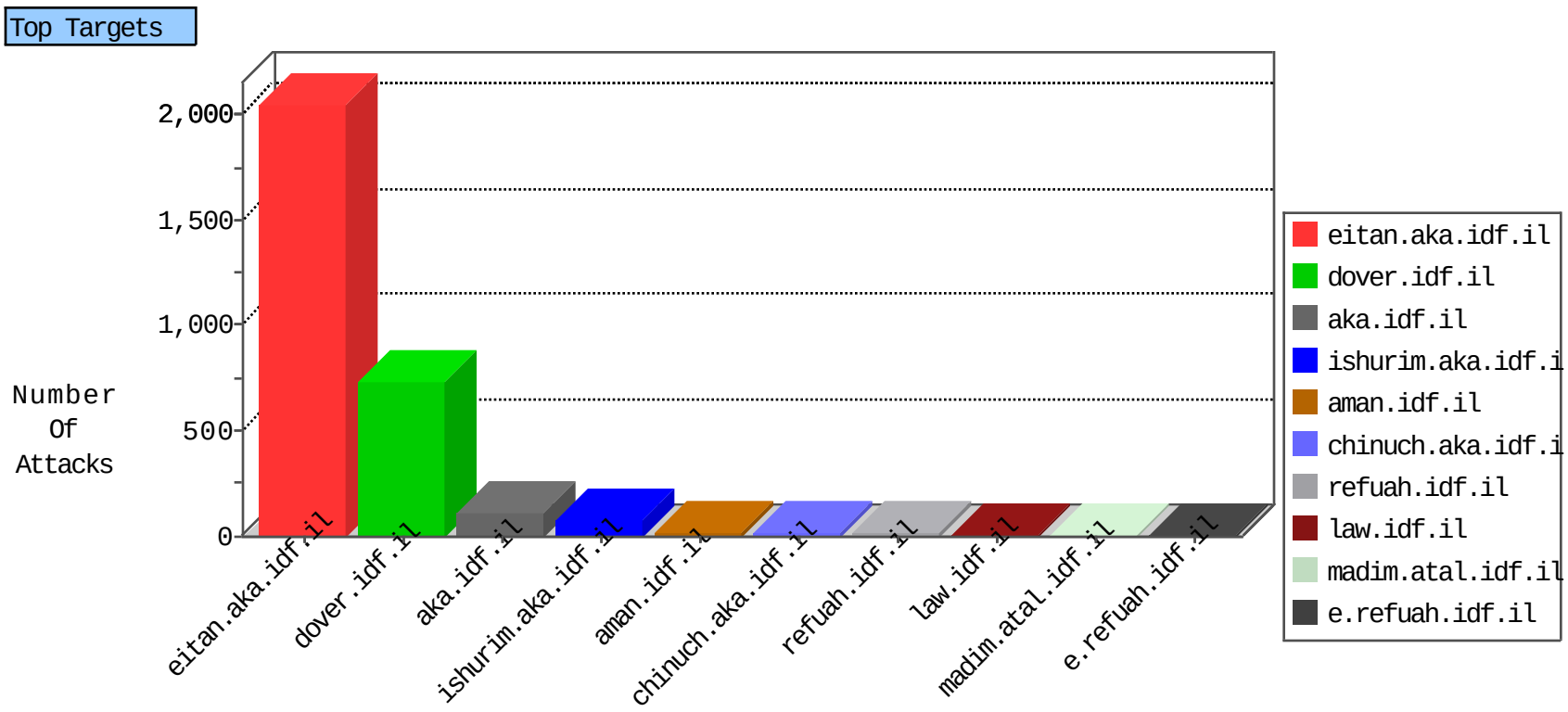
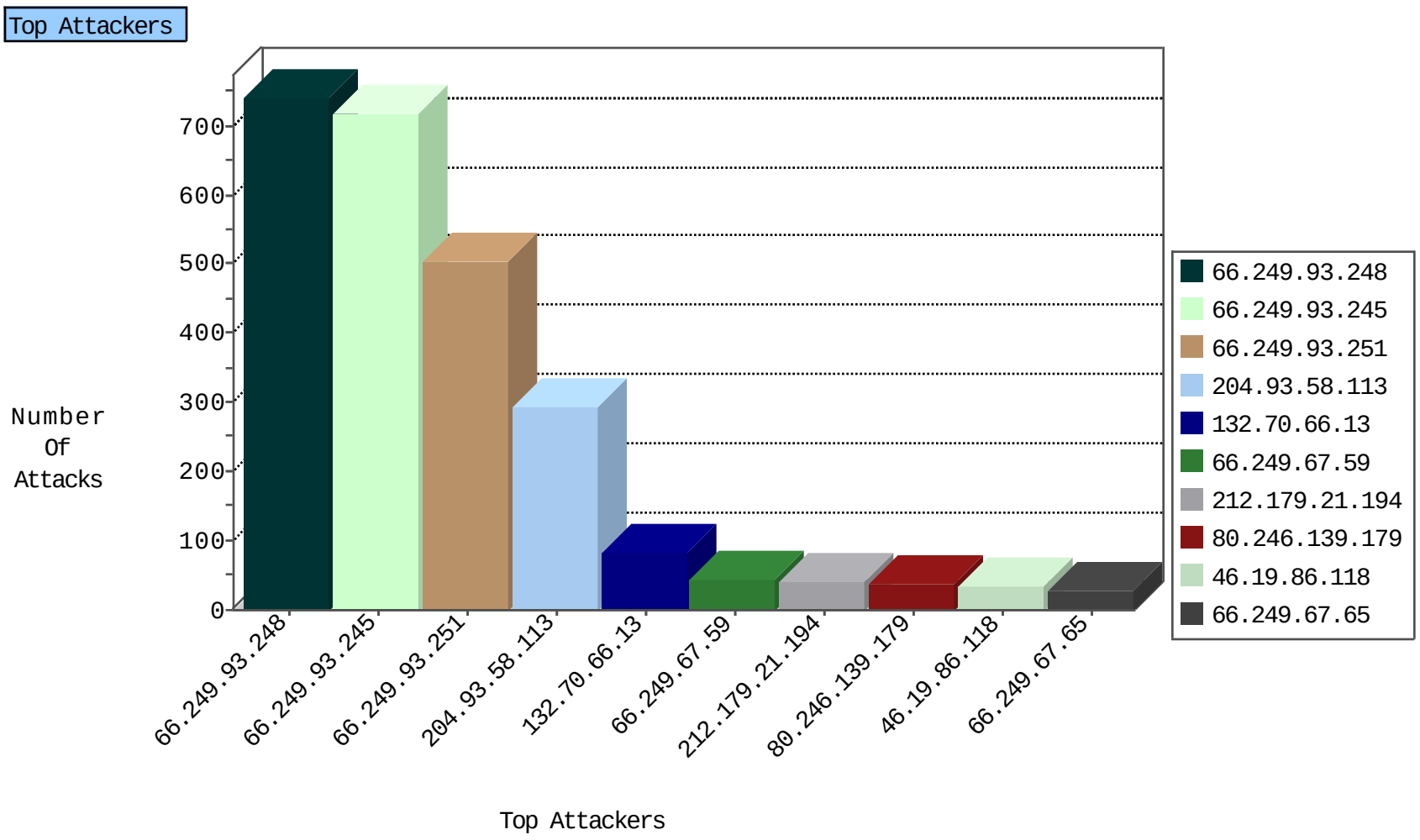
10-25-2015-14:04:05 to 10-25-2015-15:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-25-2015-14:04:05 to 10-25-2015-15:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.93.58.113	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	477302
66.249.67.59	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	124252
66.249.67.53	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	54903
66.249.67.65	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	45851
52.16.5.197	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	43927
68.180.228.112	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	18798
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	13608
41.218.182.144	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12662
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	11954
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	11538
89.13.1.19	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	10742
184.107.80.90	Canada	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	8490
105.156.35.126	Morocco	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7346
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	5743
157.166.216.10	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	4640
132.66.40.116	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2524
68.96.59.120	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1810
41.44.94.229	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	864
41.206.11.88	Nigeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	743
31.134.27.34	Russian Federation	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	500
178.255.215.87	France	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	249
157.55.39.53	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	248
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	103
80.246.139.179	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	95
46.19.86.118	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	94
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	41
77.125.4.75	Israel	147.237.72.156	aman.idf.il	Invalid TCP Flags	drop	14
80.74.100.98	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	12
93.172.59.230	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	12
31.154.25.138	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
2.54.41.212	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
37.26.149.251	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	6
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
176.13.7.111	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
217.224.122.70	Germany	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
176.12.145.110	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
89.138.74.135	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.13.108	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
92.224.201.48	Germany	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
212.179.28.34	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.13.3.155	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
31.168.219.154	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
176.13.9.163	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
213.151.53.59	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
107.77.89.76	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
185.46.212.51	Switzerland	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	3
46.19.85.195	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
46.4.10.6	Germany	147.237.76.147	chinuch.aka.idf.il	Invalid TCP Flags	drop	2
50.116.28.209	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2

10-25-2015-14:04:05 to 10-25-2015-15:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

10-25-2015-14:04:05 to 10-25-2015-15:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
211.176.108.72	147.237.77.179	Korea, Republic of	e.mazi.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.140.218.4	147.237.72.156	Kuwait	aman.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
109.65.105.29	147.237.77.216	Israel	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1

10-25-2015-14:04:05 to 10-25-2015-15:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count

10-25-2015-14:04:05 to 10-25-2015-15:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.93.248	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	728
66.249.93.245	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	718
66.249.93.251	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	504
132.70.66.13	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	84
138.134.102.16	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	14
37.26.149.203	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	14
66.249.93.248	Israel	147.237.76.200	eitan.aka.idf.il	Too Many 404: Response Code per Session	Block	14
138.134.192.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	14
37.26.149.251	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	14
192.116.94.222	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	14
66.249.64.154	Israel	147.237.76.147	chinuch.aka.idf.i	Suspicious Response Code_Custom_Temporary	Block	14
109.65.105.29	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	14
194.114.146.227	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	14

10-25-2015-14:04:05 to 10-25-2015-15:04:05