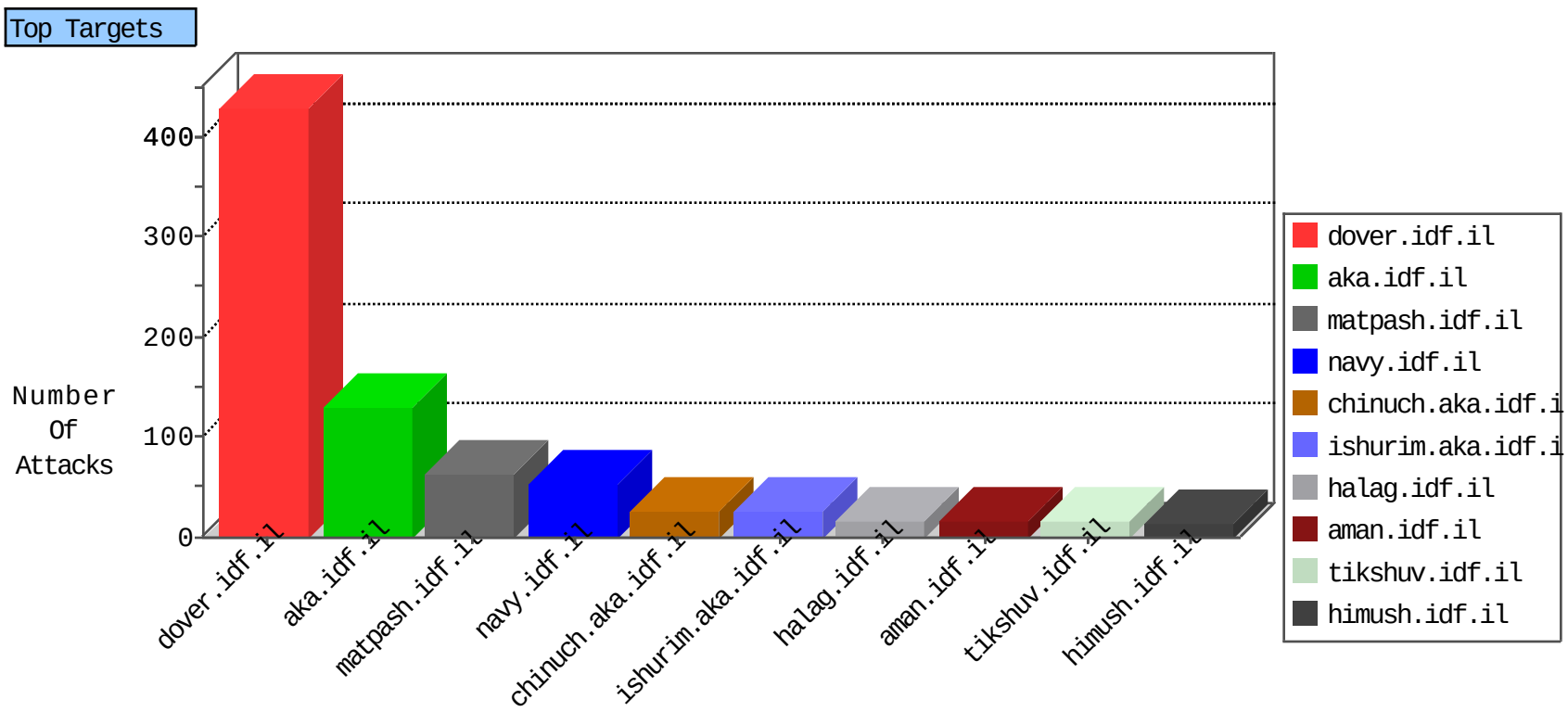
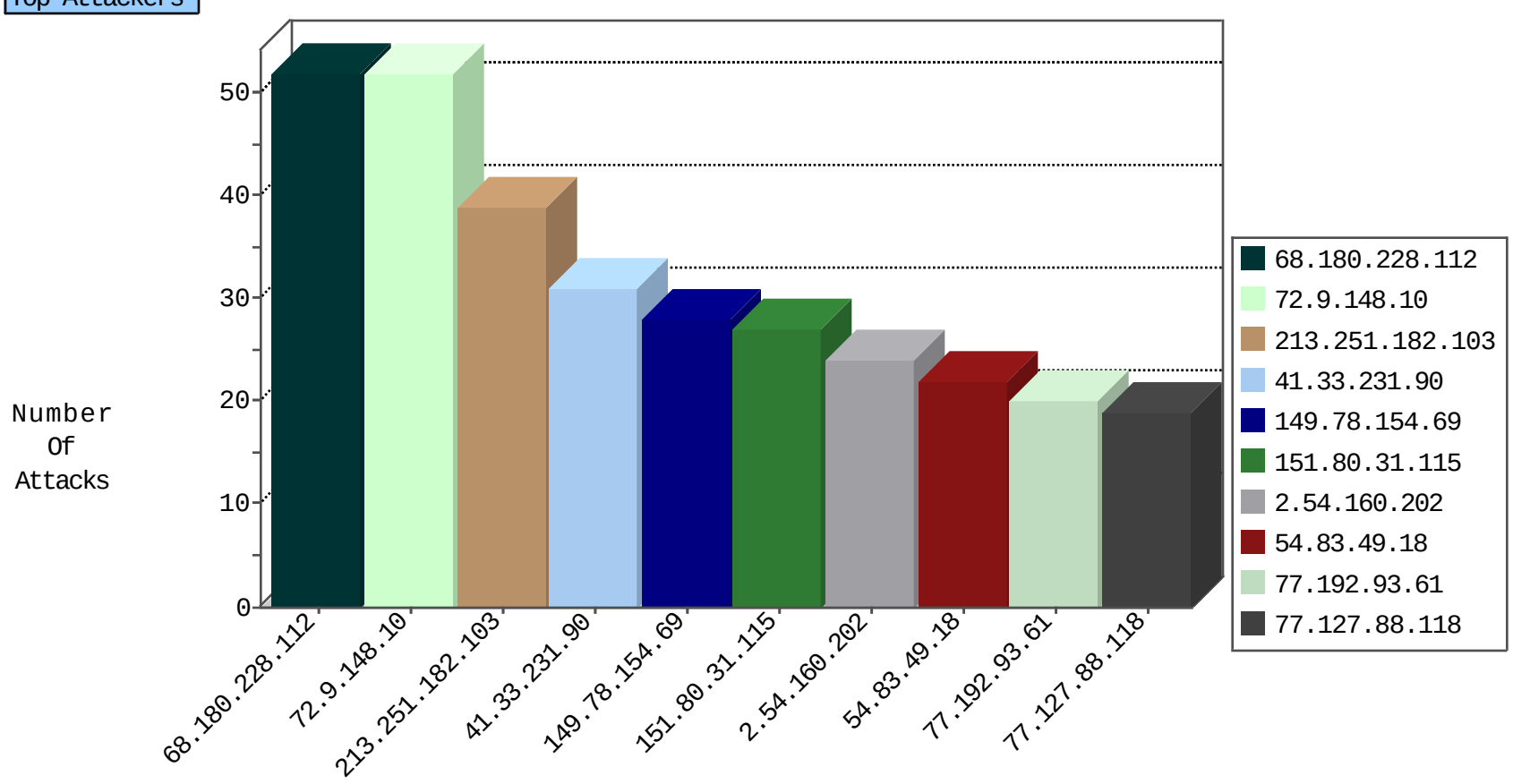
10-21-2015-01:04:07 to 10-21-2015-02:04:07

IDF Under Attack
Daily Report

Top Targets



Top Attackers



Top Attackers

10-21-2015-01:04:07 to 10-21-2015-02:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	16
77.192.93.61	France	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
109.64.176.203	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
77.127.88.118	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.60.110	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
2.54.60.110	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
93.38.247.190	Italy	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
66.249.67.59	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

10-21-2015-01:04:07 to 10-21-2015-02:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
105.102.211.160	Algeria	147.237.77.216	dover.idf.il	3807: HTTP: SQL Injection Evasion Inline SQL Comment	Block	1

10-21-2015-01:04:07 to 10-21-2015-02:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
79.143.180.44	147.237.76.39	Germany	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
5.39.222.253	147.237.77.179	Netherlands	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
209.41.67.92	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
194.54.168.76	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
107.150.55.78	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.172.201	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 1024	1
5.8.60.88	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
212.179.90.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
123.151.149.222	147.237.0.34	China	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.200.13.64	147.237.77.216	Ukraine	dover.idf.il	SERVER-WEBAPP xmlrpc.php post attempt	1

10-21-2015-01:04:07 to 10-21-2015-02:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
2.54.160.202	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
54.83.49.18	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	18
82.145.209.17	Europe	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	16
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
186.188.226.123	Panama	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
2.54.60.110	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
77.192.93.61	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.183.204.235	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
105.102.211.160	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
84.228.225.161	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
37.140.188.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
64.229.49.203	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
131.253.25.253	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.39.76	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	5
105.157.49.60	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
40.140.178.82	United States	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	5
128.232.110.28	United Kingdom	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
157.55.39.255	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.64.176.203	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.179.102.91	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.255.101	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.78.230	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.60.160	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.4.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
77.127.88.118	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.66.200.212	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
46.116.152.245	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
100.40.65.92	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.183.224.193	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
80.230.92.137	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
157.55.39.25	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
80.246.130.154	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
46.19.86.5	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
91.227.122.220	Poland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
188.165.15.126	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.179.55.169	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
66.249.67.59	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.43.112.26	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
93.38.247.190	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
151.80.31.115	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
192.235.5.61	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
178.255.215.87	France	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
66.249.67.65	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

10-21-2015-01:04:07 to 10-21-2015-02:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
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	52
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-ar/dover.aspx	Block	52
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	39
151.80.31.115	Italy	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	26
207.46.13.178	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	13
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/print_bottom.asp	Block	13
180.153.180.152	China	147.237.77.176	matpash.idf.il	URL is Above Root Directory www.cogat.idf.il/../shared/clientscripts/clientscripts.js	Block	13
50.97.52.130	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1511-en/dover.aspx&usg=alkjrhgrgvjjkoa3fo6dssqzqu5pmauyfg	Block	13
207.46.13.187	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	13
157.55.39.26	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	13
183.245.117.208	China	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
77.127.88.118	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/1110-he/tikshuv.asp/	Block	13
54.85.81.74	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mod_pagespeed_beacon	Block	13
157.55.39.211	United States	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	13
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	13
188.138.1.218	Germany	147.237.76.30	himush.idf.il	Unauthorized URL Access to 147.237.76.30/	Block	13
79.178.103.227	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	13
62.219.21.30	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	13
157.55.39.255	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/oref/	Block	13
37.142.64.103	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	13
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	13
94.230.81.216	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	13
66.249.64.239	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	13
176.13.11.113	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/talpiotquestionnaire.aspx	None	13
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	13
37.142.68.32	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https:/www.aka.idf.il/	Block	13

10-21-2015-01:04:07 to 10-21-2015-02:04:07