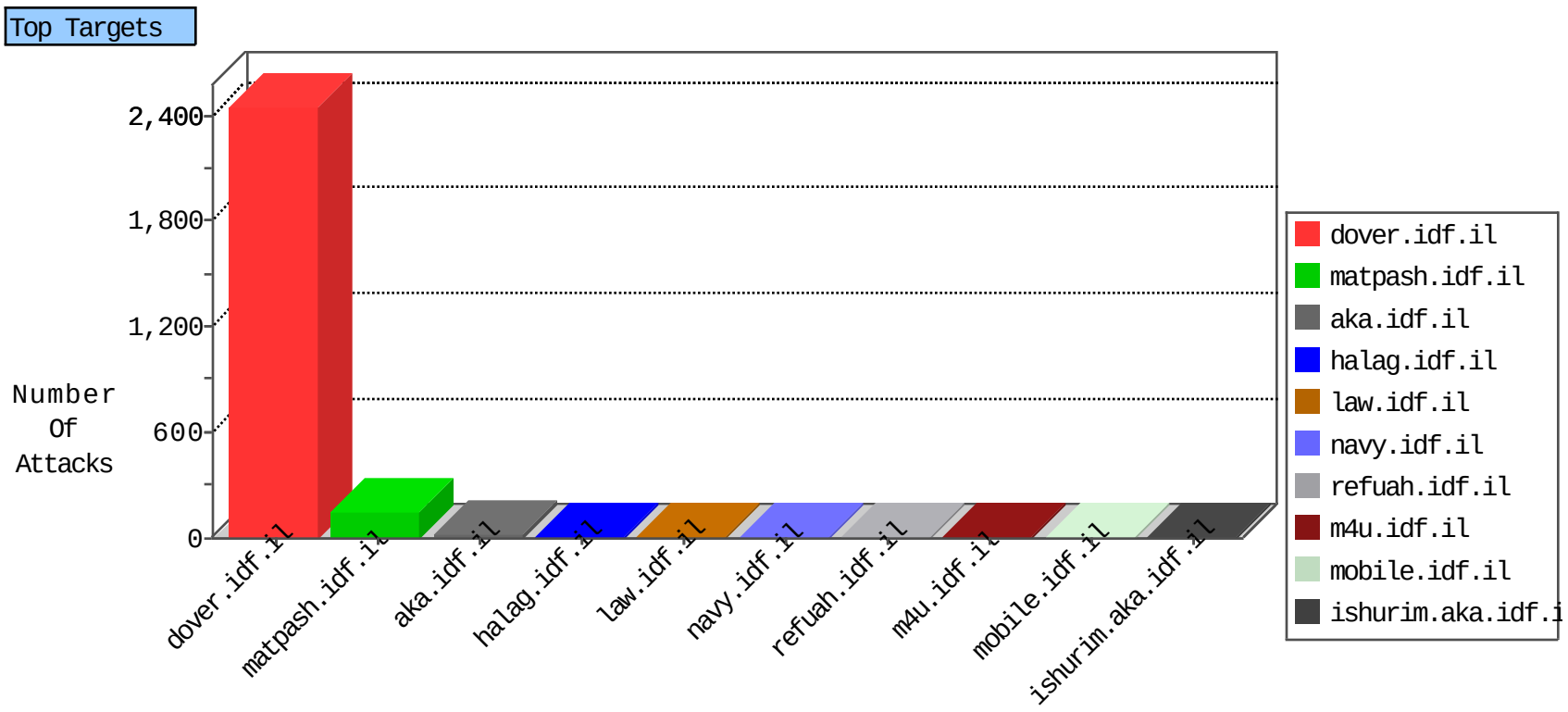
11-08-2015-03:04:08 to 11-08-2015-04:04:08

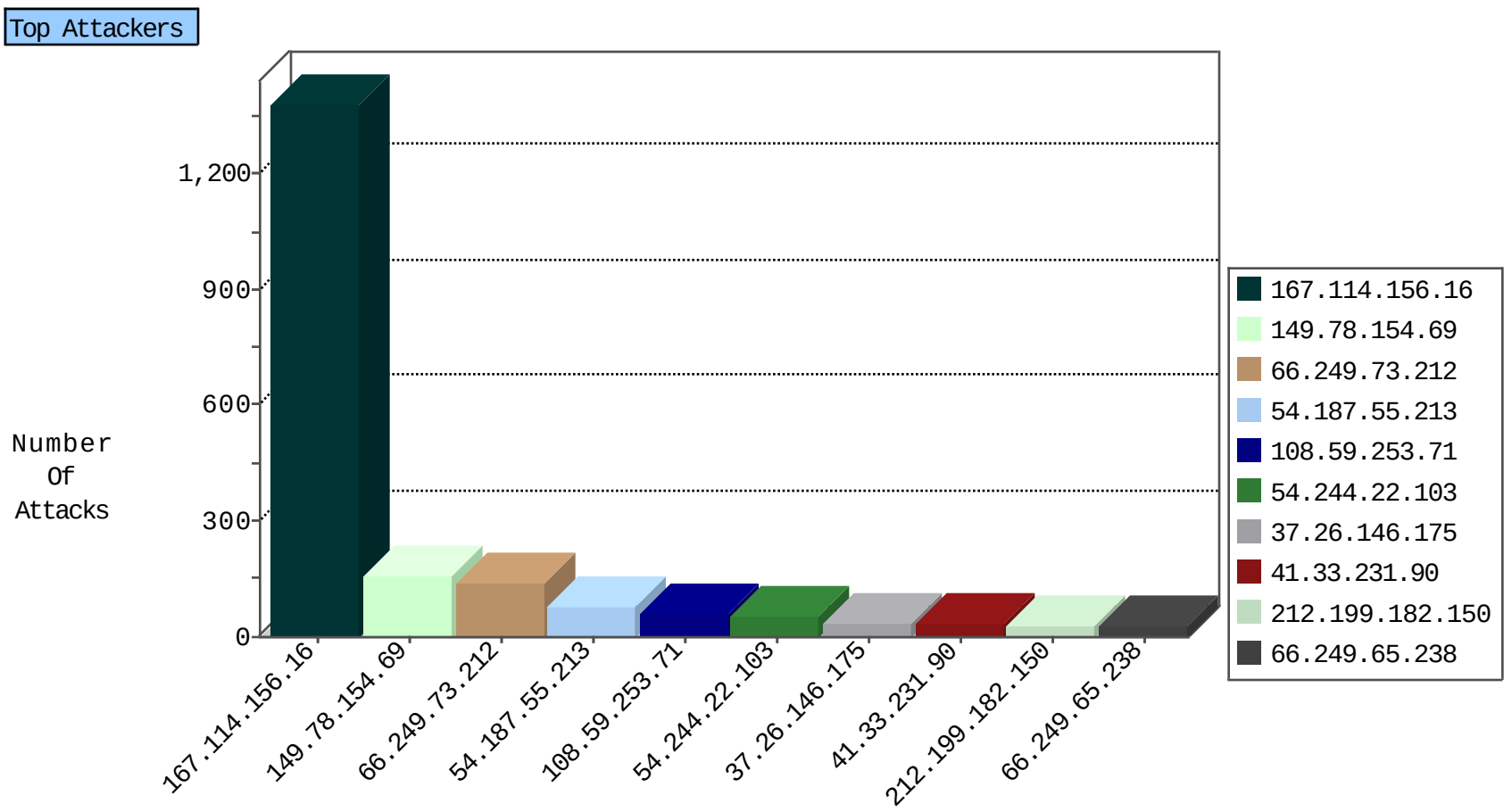
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

11-08-2015-03:04:08 to 11-08-2015-04:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2505
79.182.216.72	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	30
109.67.220.168	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
92.96.80.57	United Arab Emirates	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	1

11-08-2015-03:04:08 to 11-08-2015-04:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.9.138.211	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1

11-08-2015-03:04:08 to 11-08-2015-04:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.73.212	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	140
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
41.96.27.171	147.237.77.216	Algeria	dover.idf.il	ET WEB_SERVER Script tag in URI, Possible Cross Site Scripting Attempt	2
41.96.27.171	147.237.77.216	Algeria	dover.idf.il	ET WEB_SERVER /system32/ in Uri - Possible Protected Directory Access Attempt	2
41.96.27.171	147.237.77.216	Algeria	dover.idf.il	SQL Injection - Select From	2
41.96.27.171	147.237.77.216	Algeria	dover.idf.il	SERVER-IIS cmd.exe access	2
41.96.27.171	147.237.77.216	Algeria	dover.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	2
41.96.27.171	147.237.77.216	Algeria	dover.idf.il	ET WEB_SERVER cmd.exe In URI - Possible Command Execution Attempt	2
41.96.27.171	147.237.77.216	Algeria	dover.idf.il	ET WEB_SERVER Possible SQL Injection Attempt SELECT FROM	2
41.96.27.171	147.237.77.216	Algeria	dover.idf.il	ET WEB_SERVER /bin/sh In URI Possible Shell Command Execution Attempt	2
41.96.27.171	147.237.77.216	Algeria	dover.idf.il	SQL url ending in comment characters - possible sql injection attempt	2
41.96.27.171	147.237.77.216	Algeria	dover.idf.il	SERVER-WEBAPP /etc/passwd file access attempt	2
41.96.27.171	147.237.77.216	Algeria	dover.idf.il	POLICY-OTHER script tag in URI - likely cross-site scripting attempt	2
41.96.27.171	147.237.77.216	Algeria	dover.idf.il	GPL WEB_SERVER /etc/passwd	2
198.52.97.85	147.237.77.216	United States	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
188.138.9.51	147.237.76.176	Germany	test.ncore.idf.i	ET SCAN NMAP -sS window 1024	1
27.147.156.5	147.237.0.200	Bangladesh	m4u.idf.il	ET SCAN NMAP -sS window 3072	1
27.147.156.5	147.237.0.200	Bangladesh	m4u.idf.il	ET SCAN NMAP -f -sS	1
31.6.71.154	147.237.76.197	Poland	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
120.107.144.49	147.237.72.156	Taiwan	aman.idf.il	ET SCAN NMAP -sS window 1024	1
27.147.156.5	147.237.0.200	Bangladesh	m4u.idf.il	ET SCAN NMAP -sS window 2048	1

11-08-2015-03:04:08 to 11-08-2015-04:04:08

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.i	drop	First packet isn't SYN	drop	155
54.187.55.213	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	75
108.59.253.71	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	61
54.244.22.103	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	51
37.26.146.175	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
212.199.182.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	29
82.192.68.46	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	27
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
62.83.140.53	Spain	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
142.161.71.252	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
12.250.192.226	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	23
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	21
66.249.65.238	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	20
185.26.182.37	Europe	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
99.224.238.30	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
104.34.185.61	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
100.100.7.188		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
66.102.8.238	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
40.77.167.9	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
212.179.90.106	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
82.80.25.221	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	10
66.249.65.238	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
208.115.111.73	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	9
66.249.65.231	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
176.13.15.153	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
157.55.39.31	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	8
157.55.39.175	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	7
66.102.8.233	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	SAM rule	drop	6
96.59.65.90	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
79.182.216.72	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
208.115.113.89	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
66.249.65.224	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.109.235.140	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
173.214.173.227	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
157.55.39.24	United States	147.237.77.234	halag.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
40.77.167.67	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	6
46.19.85.119	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
125.254.18.78	Australia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	5
40.77.167.20	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	5
157.55.39.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	5
69.65.79.111	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	5
195.34.150.18	Austria	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	5
64.233.172.163	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	5

11-08-2015-03:04:08 to 11-08-2015-04:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.115.111.72	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	6
107.150.56.165	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.cloud.ph/	Block	1
64.19.78.242	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
188.165.15.14	France	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	1
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
109.64.108.28	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/login.aspx	Block	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/1528.png	Block	1
207.46.13.102	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	1
66.249.67.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
37.26.146.175	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
157.55.39.24	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/civiladministration/govermment/pages/justice1.asp	Block	1
66.249.64.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8853-he/refuah.aspx	Block	1
67.212.175.138	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/yohalan/main/main.asp	Block	1
37.26.149.128	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
157.55.39.141	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19396-he/idfgdover.aspx	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1414-he/dover.aspx	Block	1
46.121.40.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
157.55.39.248	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1

11-08-2015-03:04:08 to 11-08-2015-04:04:08