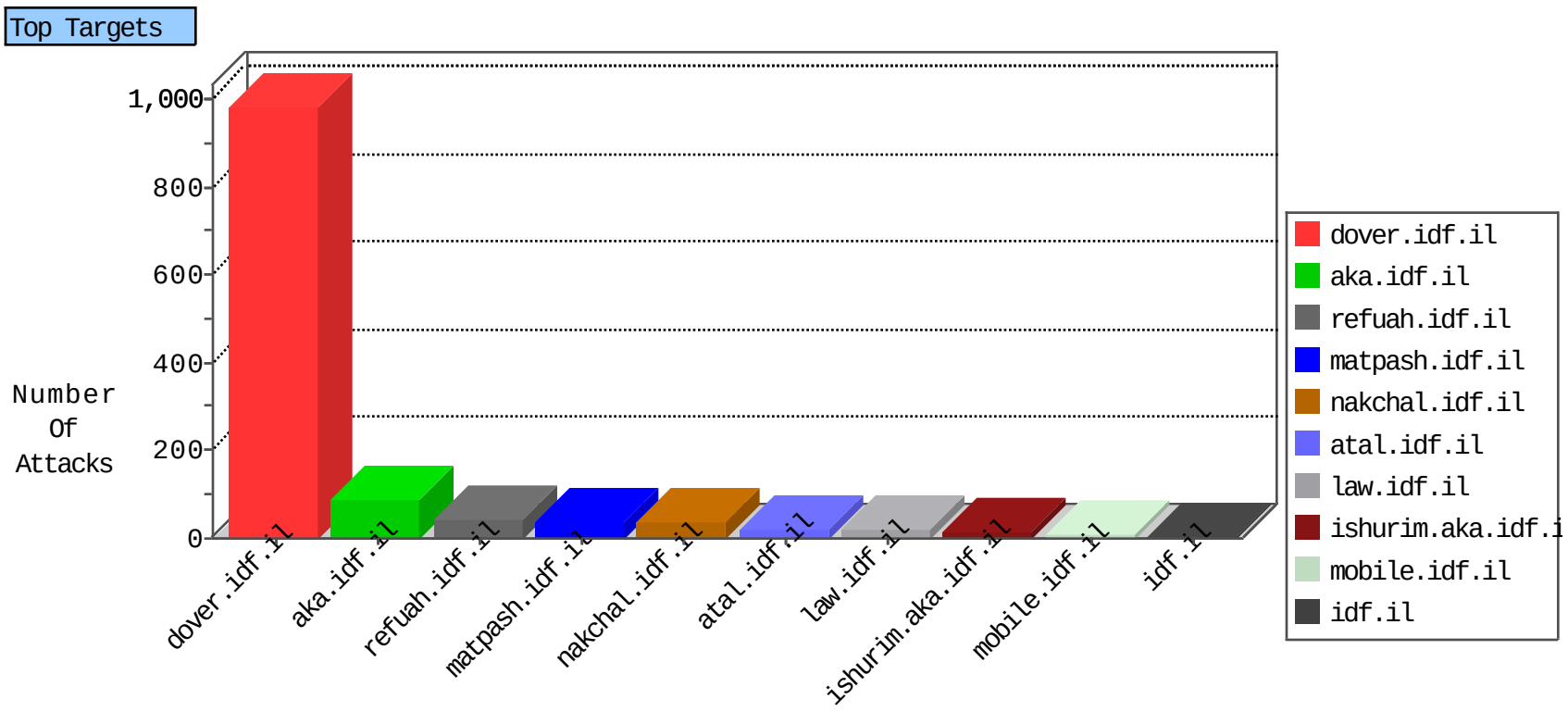
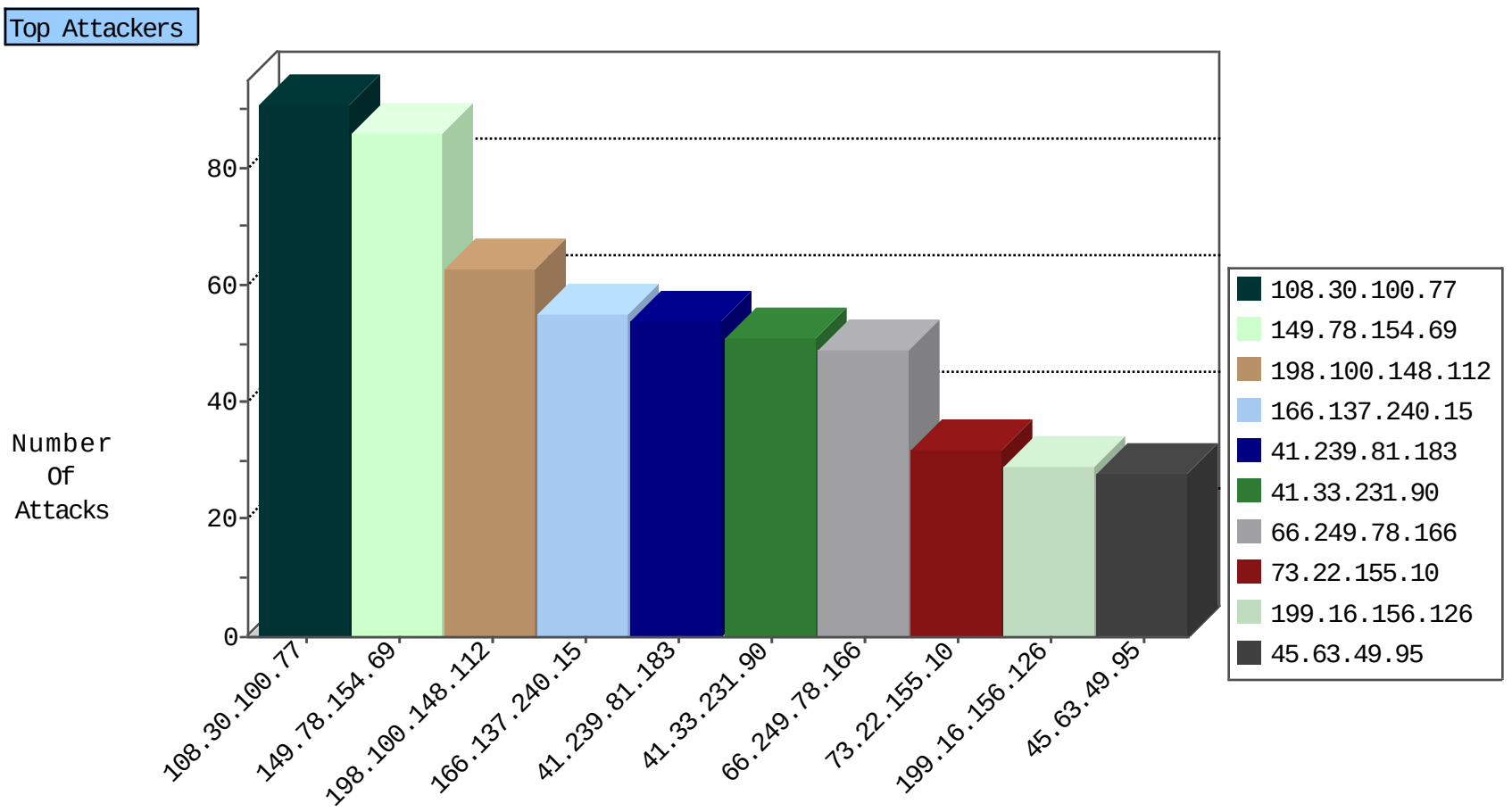
10-28-2015-03:04:00 to 10-28-2015-04:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-28-2015-03:04:00 to 10-28-2015-04:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.103.159.119	Algeria	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
204.42.253.2	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
5.8.66.69	Russian Federation	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1

10-28-2015-03:04:00 to 10-28-2015-04:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
222.84.5.158	China	147.237.76.31	nakchal.idf.il	C1000108: HTTP: Trying to locate existing FCKeditor	Block	4

10-28-2015-03:04:00 to 10-28-2015-04:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
94.102.48.194	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1
79.180.116.223	147.237.77.170	Israel	maarachot.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
210.50.197.147	147.237.72.167	Australia	ishurim.aka.idf.i	ET SCAN NMAP -sS window 3072	1
186.209.188.248	147.237.8.24	Brazil	e.lifestyle.idf.i	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
120.150.29.211	147.237.76.38	Australia	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
95.154.229.204	147.237.77.216	United Kingdom	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	1
92.247.120.60	147.237.72.14	Bulgaria	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	1
120.150.29.211	147.237.76.38	Australia	e.e.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
117.38.218.35	147.237.76.31	China	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

10-28-2015-03:04:00 to 10-28-2015-04:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
108.30.100.77	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	91
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	86
198.100.148.112	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	63
166.137.240.15	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	55
41.239.81.183	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	54
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
51.39.109.218	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
41.103.159.119	Algeria	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	First packet isn't SYN	drop	20
82.132.217.71	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.84.165	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.102.8.173	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
131.253.25.255	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
5.67.3.33	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
108.59.253.71	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.248	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	7
147.9.80.163	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	7
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	7
66.249.78.166	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
40.77.167.36	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
173.212.172.6	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.84.167	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.241.237.163	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.4.155	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.81	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
71.81.128.86	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
94.228.34.248	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.39.41	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
73.22.155.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.201	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
46.121.94.141	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.4.10.6	Germany	147.237.76.147	chinuch.aka.idf.il	drop	First packet isn't SYN	drop	3
66.102.8.168	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.67.34	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.4.155	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
50.153.129.37	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
99.237.228.221	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

10-28-2015-03:04:00 to 10-28-2015-04:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.64.205.157	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 85.64.205.157	Block	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	14
45.63.49.95		147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/	Block	14
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/6/size220x0/17436.jpg	Block	14
73.22.155.10	United States	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	14
66.249.75.16	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	14
94.242.246.23	Luxembourg	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	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	14
66.168.208.221	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.168.208.221	Block	14
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/6/size220x0/17436.jpg	Block	14
73.22.155.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/	Block	14
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	14
141.212.122.160	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/	Block	14
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/idf/templates/innerpage.aspx	Block	14
66.168.208.221	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/3896.pdf++972+oil+furniture+building+company@.com+il&as_qdr=all&filter=0&num=100&complete=0&cr=countryil&gws_rd=ssl&hl=iw&&ct=clnk	Block	14
199.16.156.126	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/9/size220x0/17429.jpg	Block	14
79.181.58.67	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	14
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-18489-he/dover.aspx	Block	14
37.142.68.53	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	14
157.55.39.11	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	14
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	14
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1164-he/chinuch.aspx	Block	14
79.181.58.67	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	14
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	14
45.63.49.95		147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to 147.237.72.167/	Block	14
188.165.15.130	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	14
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/robots.txt	Block	14
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	14

10-28-2015-03:04:00 to 10-28-2015-04:04:00