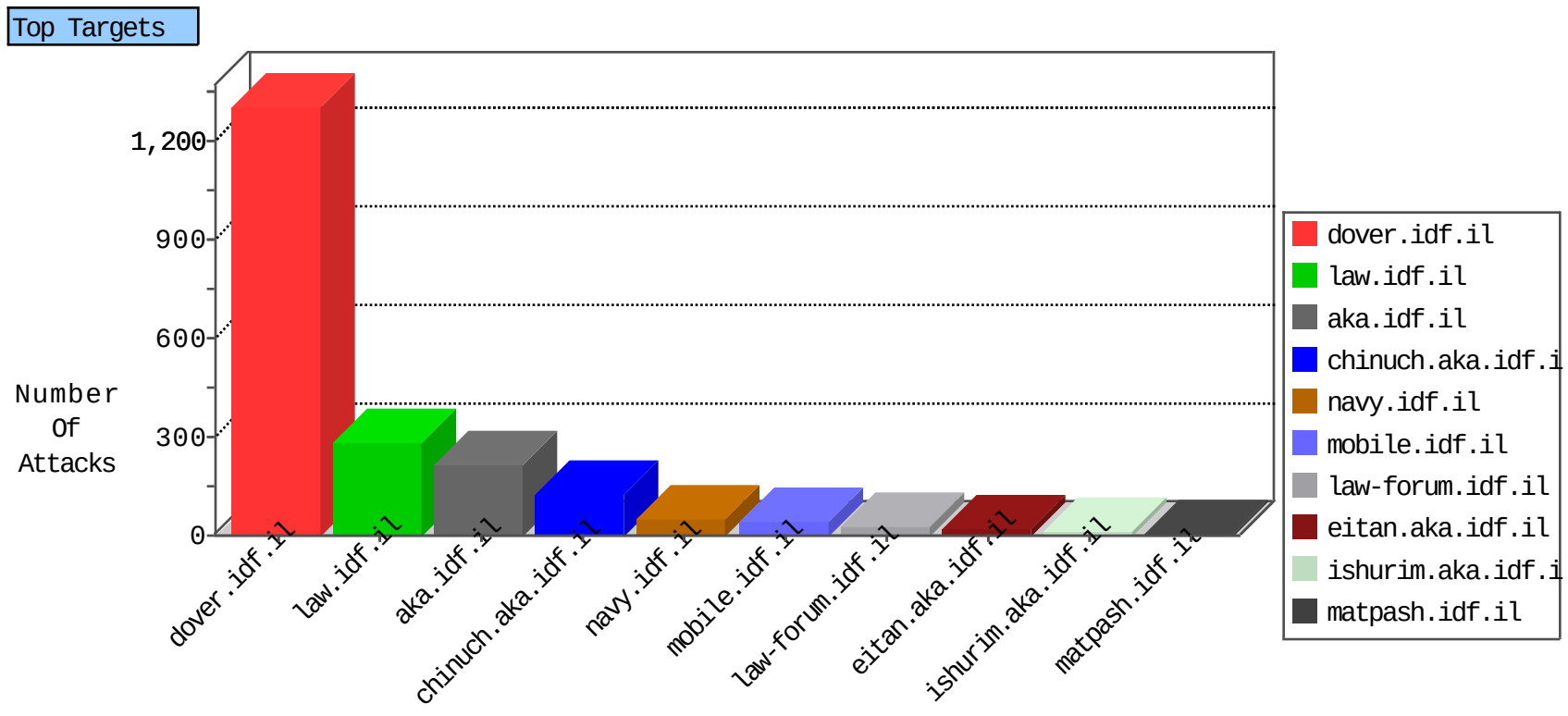
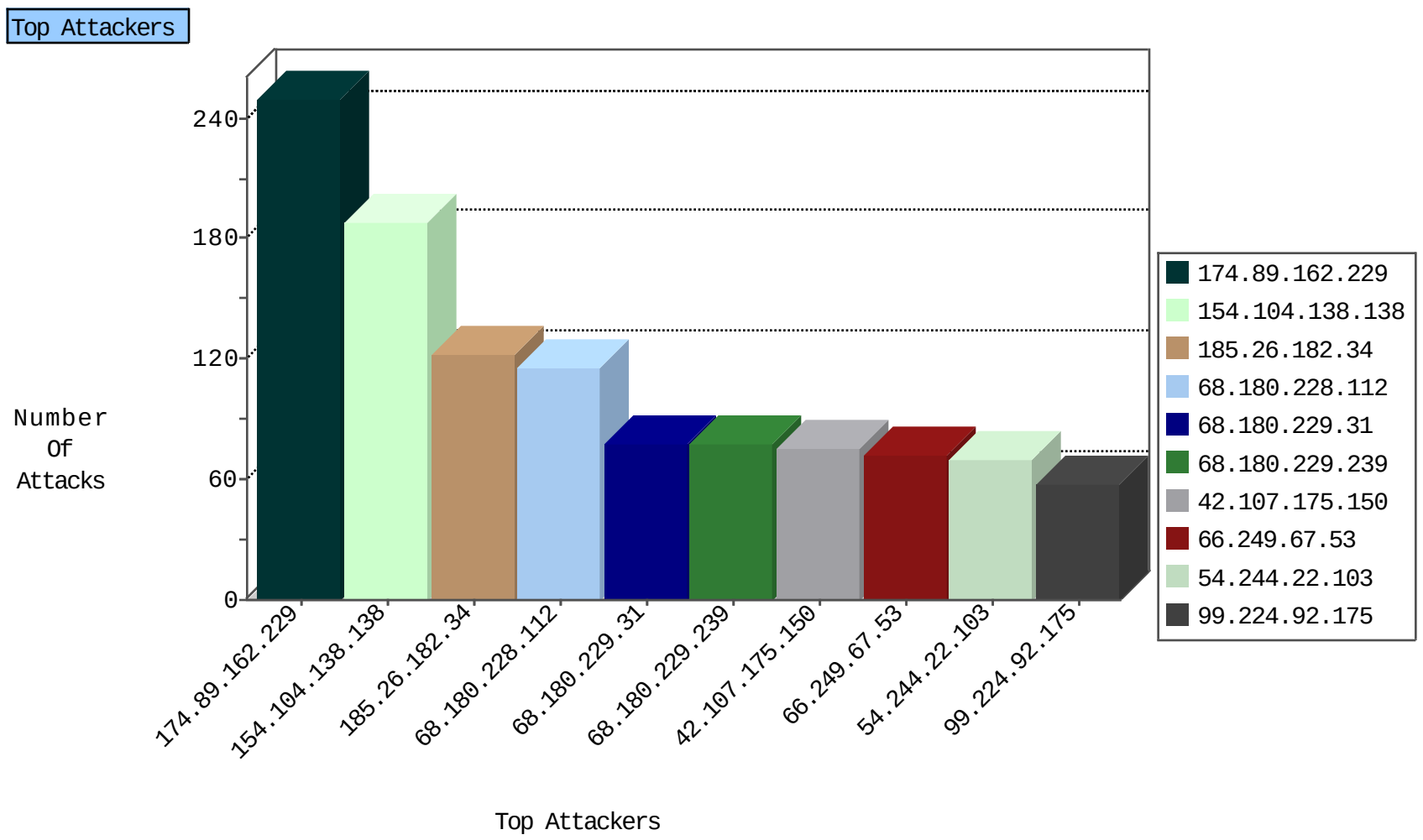
10-20-2015-03:04:04 to 10-20-2015-04:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-20-2015-03:04:04 to 10-20-2015-04:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
115.239.228.8	China	147.237.76.42	refuah.idf.il	JLM_Under_Attack_Con_Http	drop	2
114.112.90.54	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
71.6.165.200	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
93.174.93.100	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

10-20-2015-03:04:04 to 10-20-2015-04:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.229.107.227	Israel	147.237.72.166	aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
138.47.27.43	United States	147.237.77.74	law.idf.il	C008: HTTP: Xenu UserAgent	Block	1

10-20-2015-03:04:04 to 10-20-2015-04:04:04

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	12
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
77.236.96.52	147.237.8.50	Germany	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1

10-20-2015-03:04:04 to 10-20-2015-04:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
154.104.138.138	Tunisia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	188
185.26.182.34	Europe	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	122
174.89.162.229	Canada	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	109
42.107.175.150	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	75
99.224.92.175	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	50
46.19.86.121	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	46
79.129.43.130	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
70.81.128.224	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
188.143.232.24	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
82.192.68.46	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
54.244.22.103	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	24
157.55.81.9	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
37.26.148.225	Israel	147.237.76.200	eitan.aka.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	SAM rule	drop	11
109.64.1.215	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
87.68.241.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
93.172.184.58	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
178.152.57.121	Qatar	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
219.74.36.64	Singapore	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.67.65	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
66.249.67.59	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
109.64.1.215	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	drop	First packet isn't SYN	drop	7
212.199.182.150	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
41.225.19.17	Tunisia	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	7
37.140.188.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
118.210.76.216	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.242.37.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.72.0.55	Ireland	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
66.249.67.53	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.65.146.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
199.203.67.223	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.227.118.21	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.81.215	Russian Federation	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.109.98.237	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.54.13.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
177.83.193.99	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.39.237	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.67.59	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
176.205.61.144	United Arab Emirates	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
66.249.67.122	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
107.178.209.181	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
174.89.162.229	Canada	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/565-en/patzar.aspx	Block	141
68.180.229.31	United States	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	78
68.180.229.239	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	78
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in URL from 68.180.228.112	Block	65
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	52
75.23.196.15	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	52
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	39
72.9.148.10	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	39
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1397-en/dover.aspx	Block	26
66.249.67.122	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	26
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
176.13.19.9	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 176.13.19.9	Block	13
77.237.138.51	Czech Republic	147.237.77.19	law-forum.idf.il	Distributed Unauthorized URL Access on /	Block	13
92.225.35.231	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
68.196.137.237	United States	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/viewpniot.aspx	None	13
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/bin	Block	13
176.13.19.9	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	13
77.237.138.202	Czech Republic	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to /	Block	13
133.130.48.124	Japan	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/8/888.pdf	Block	13
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	13
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/homefront/kkkkkkk=cd07c66ckkkkkkk_cd07c66c	Block	13
85.64.205.157	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	13
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	13
151.80.31.141	Italy	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/14-he	Block	13
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	13
188.143.232.24	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/article.in.aspx/templates/sendtofriend/sendtofriend.aspx	Block	13
88.75.185.185	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Suspicious Response Code	Block	13
68.180.228.112	United States	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL /mivtza>×¡×Ÿ×•×¦×˜×?×›Ã¼×?×žœ ×¡×?×™×¢×•, ×¡×žפ×?×?×?×žœ ×″×›Ã¿ â€Ž×¢×˜×¥ ×¦×•×› ×•×™. <table cellspacing=	Block	13
198.20.69.74	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	13
91.55.188.12	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
68.196.137.237	United States	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in aka.idf.il/main/sachar/viewpniot.aspx	None	13