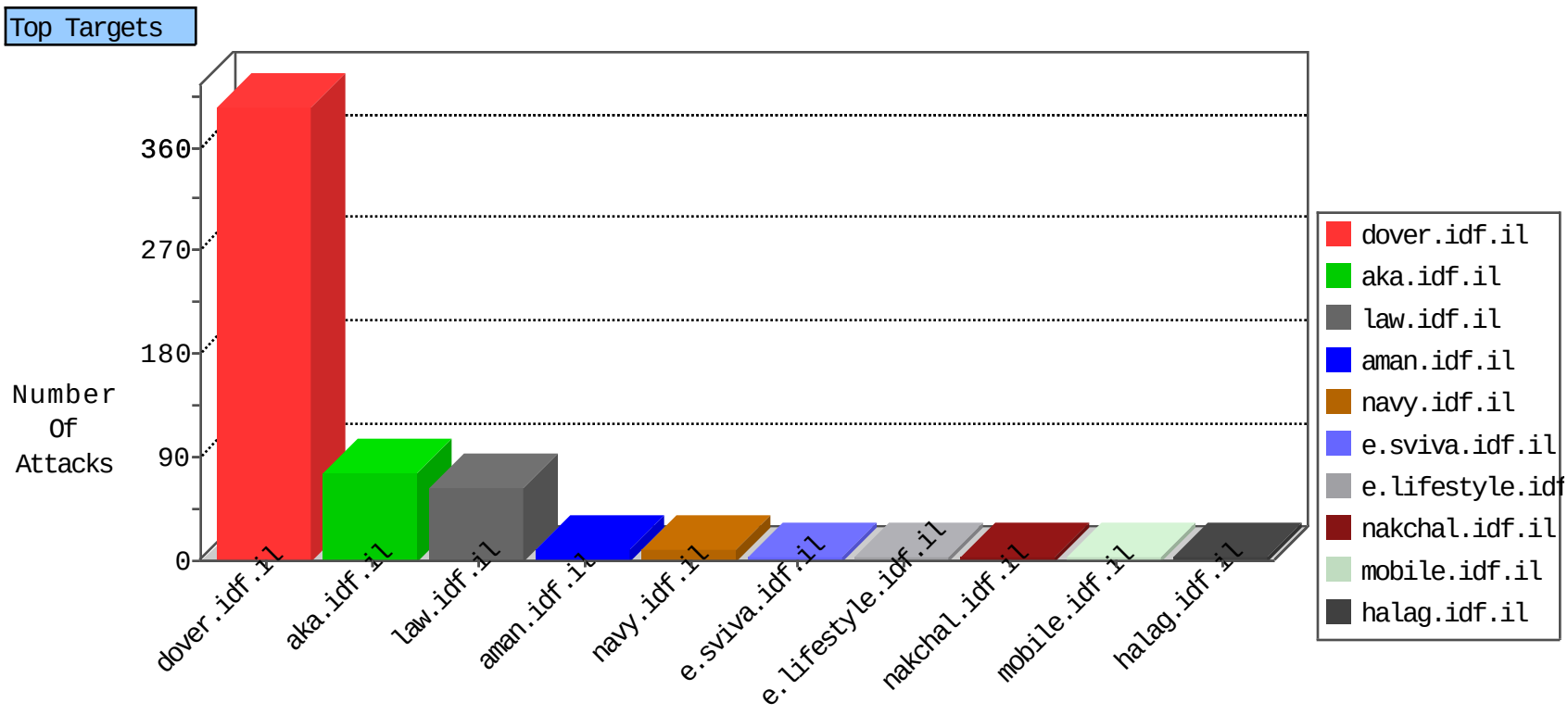
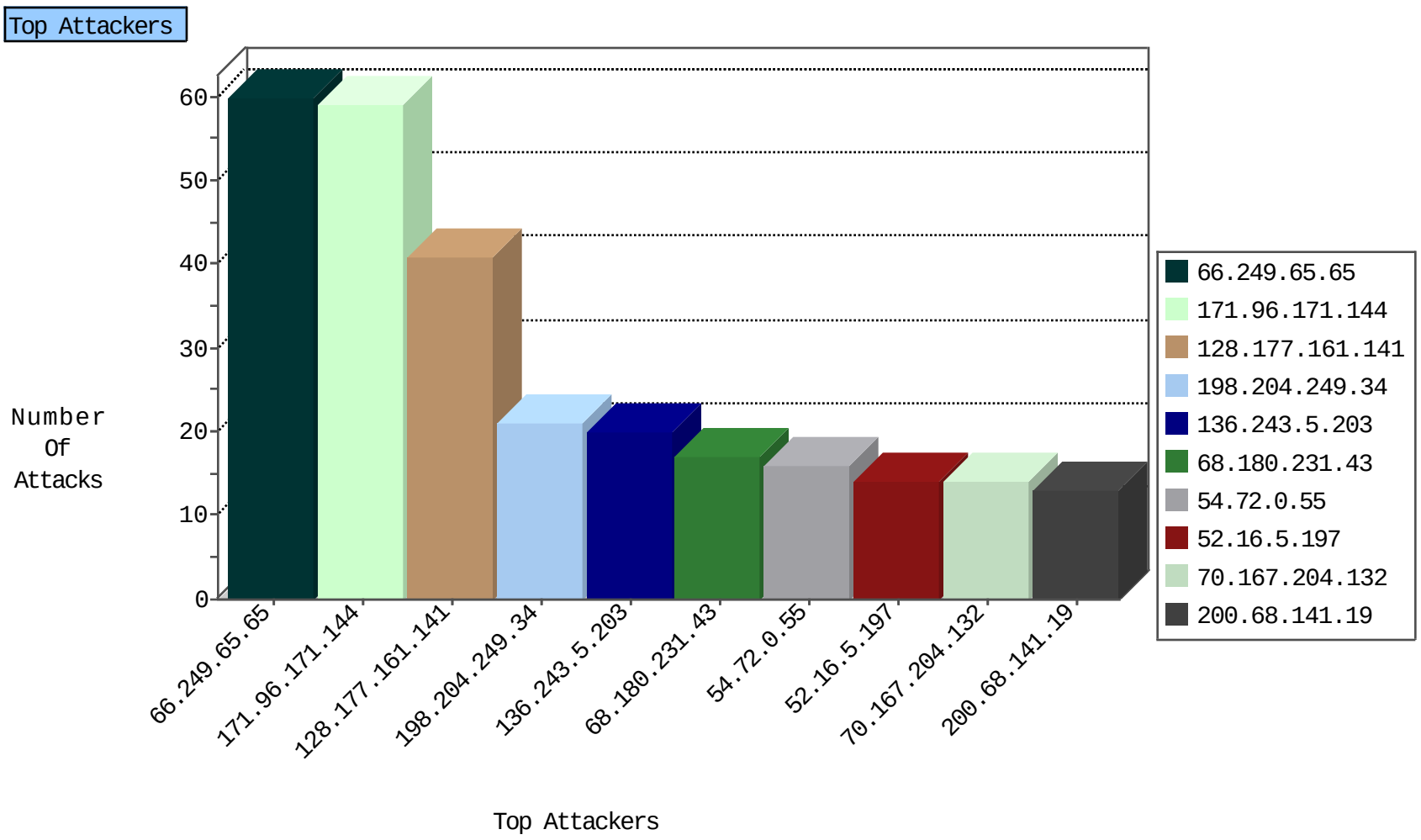
04-22-2016-04:04:01 to 04-22-2016-05:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-22-2016-04:04:01 to 04-22-2016-05:04:01

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	3
204.42.253.2	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	2
94.102.52.10	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
94.102.52.10	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
188.138.1.218	Germany	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1

04-22-2016-04:04:01 to 04-22-2016-05:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-22-2016-04:04:01 to 04-22-2016-05:04:01

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	10
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
188.138.25.228	147.237.8.46	France	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	2
109.235.254.181	147.237.76.197	Turkey	e.himush.idf.il	ET SCAN NMAP -sS window 2048	1
104.171.122.176	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
13.92.246.145	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 2048	1
212.129.15.245	147.237.77.243	France	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
139.196.57.234	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -sS window 1024	1
109.235.254.181	147.237.76.197	Turkey	e.himush.idf.il	ET SCAN NMAP -sS window 4096	1
109.235.254.181	147.237.76.197	Turkey	e.himush.idf.il	ET SCAN NMAP -f -sS	1
104.171.122.176	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 3072	1
13.92.246.145	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -sS window 4096	1
13.92.246.145	147.237.77.234	United States	halag.idf.il	ET SCAN NMAP -f -sS	1
188.138.25.228	147.237.8.46	France	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
115.47.12.162	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1

04-22-2016-04:04:01 to 04-22-2016-05:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.65.65	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
171.96.171.144	Thailand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
128.177.161.141	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	41
198.204.249.34	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
136.243.5.203	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
70.167.204.132	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
200.68.141.19	Mexico	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
198.58.103.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
106.38.241.106	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
185.61.138.125	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.130	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.135	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
85.134.55.152	Finland	147.237.8.24	e.lifestyle.idf	Geo-location enforcement	Geo-location inbound enforcement	drop	4
8.37.227.69	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
87.106.184.160	Germany	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
66.249.64.233	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
185.3.147.101	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
172.58.169.134	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
207.46.13.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
104.233.83.9	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
157.55.39.243	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
212.179.212.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.216	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.46.13.180	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
31.210.187.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
174.129.237.157	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
192.243.55.134	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
104.233.83.9	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
192.243.55.134	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.131	United States	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	2
128.242.249.12	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.136	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
192.243.55.135	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
68.180.231.43	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
192.243.55.137	United States	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
173.252.90.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
192.243.55.133	United States	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

04-22-2016-04:04:01 to 04-22-2016-05:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	6
66.102.8.238	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
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	2
66.102.8.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
207.46.13.99	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
207.46.13.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
107.133.32.146	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.64.124	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/main/giyus/general.aspx	Block	1
74.82.47.2	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
192.243.55.130	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/undefined	Block	1
207.46.13.180	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-8517-he/atal.aspx	Block	1
66.102.8.243	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
198.58.103.92	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
66.249.65.217	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/registrationwizard/register.aspx	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 106.38.241.106	Block	1
66.249.64.119	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 66.249.64.119	Block	1
207.46.13.10	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.134	Israel	147.237.0.34	tikshuv.idf.il	Distributed Unauthorized URL Access on www.tikshuv.idf.il/main/giyus/general.aspx	Block	1
45.32.239.214	Netherlands	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/jpg/image.jpg	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-10023-en	Block	1
66.249.64.119	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1

04-22-2016-04:04:01 to 04-22-2016-05:04:01