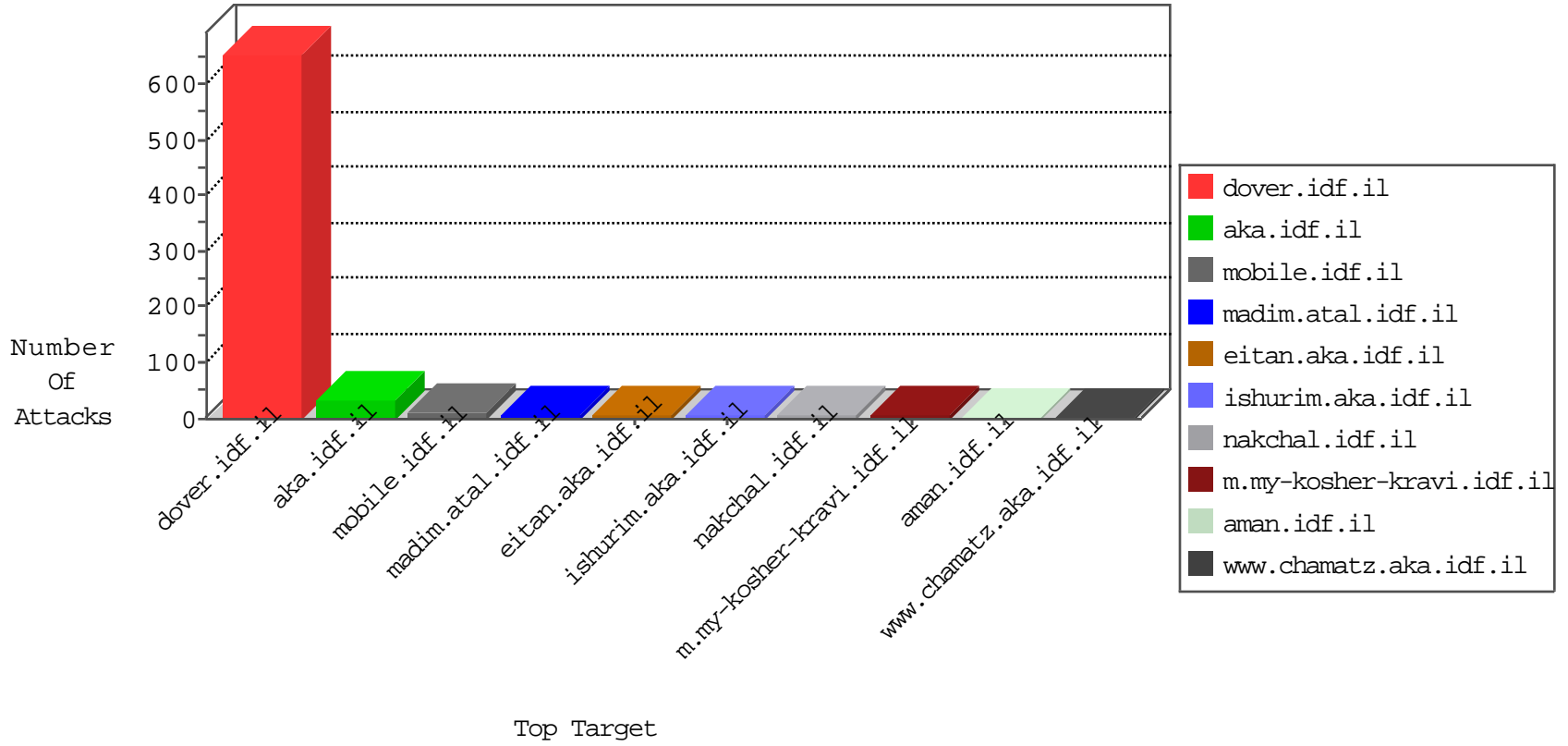


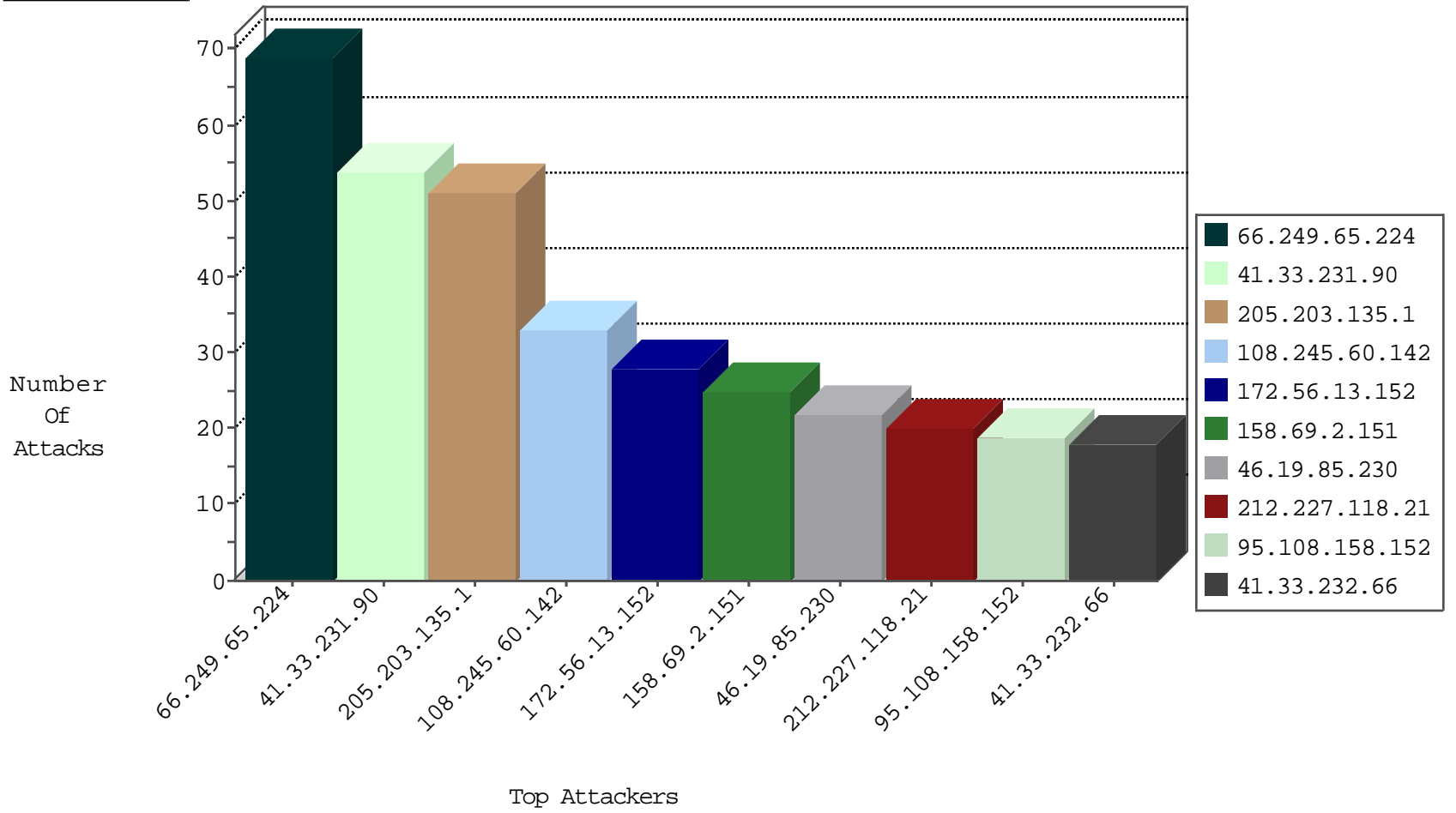
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	5
198.20.69.98	United States	147.237.76.198	e.ychalan.idf.il	Block_Ntp_All_Net	drop	1
71.6.165.200	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
176.123.29.54	Moldova, Republic of	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1

11-21-2015-04:04:01 to 11-21-2015-05:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

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
184.172.196.106	147.237.77.179	United States	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
184.172.196.106	147.237.77.170	United States	maarachot.idf.il	ET SCAN Potential SSH Scan	1
158.69.212.206	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential SSH Scan	1
120.72.118.85	147.237.0.17	Vietnam	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
184.172.196.106	147.237.77.176	United States	matpash.idf.il	ET SCAN Potential SSH Scan	1
184.172.196.106	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
123.188.125.126	147.237.0.33	China	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
88.249.106.23	147.237.77.227	Turkey	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
205.203.135.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
66.249.65.224	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	48
108.245.60.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	29
158.69.2.151	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
212.227.118.21	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
95.108.158.152	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
24.114.23.179	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
172.56.13.152	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
172.56.13.152	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
5.255.253.168	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
95.108.158.171	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.96	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.100.1.241		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
139.162.216.112	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
5.255.253.158	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.96.215	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
46.19.85.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
5.255.253.150	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
195.34.150.18	Austria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
37.140.141.2	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
98.210.37.154	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
37.201.171.7	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
157.55.39.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
40.77.167.102	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
157.55.39.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	7
109.200.30.168	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.255.253.157	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
70.215.132.198	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
199.16.156.124	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.39.132	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
199.16.156.125	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
65.55.210.92	United States	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
208.99.231.239	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
84.110.7.115	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
168.63.137.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.65.22	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.236.24.53	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
195.154.226.90	France	147.237.72.166	aka.idf.il	drop	SAM rule	drop	3
79.182.117.12	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.254.158.75	Latvia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.224	Block	14
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.231	Block	7
66.249.65.238	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.238	Block	6
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	5
176.12.146.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.255.253.168	Russian Federation	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
40.77.167.102	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
157.55.39.35	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
2.54.173.115	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
95.108.158.171	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/homefront	Block	1
68.180.230.167	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in nakchal.idf.il/1117-he/nakhal.aspx	Block	1
207.46.13.127	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/civiladministration/minhalnews/pages/hakalahom.aspx	Block	1
115.230.126.48	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/ckfinder	Block	1
84.94.161.105	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Double URL Encoding - parameter: returnUrl in m.my-kosher-kravi.idf.il/templates/login.aspx	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
107.150.43.206	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to /	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakchal.idf.il/1111-he/nakhal.aspx	Block	1
207.46.13.158	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sachar/forms/downloadform.asp	Block	1
141.212.122.160	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to 147.237.72.156/	Block	1
85.10.210.199	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
216.218.206.66	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
66.249.67.251	Israel	147.237.72.166	aka.idf.il	Unknown Parameter 5cf35968 in aka.idf.il/news/	None	1
203.133.171.95	Korea, Republic of	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
31.193.51.17	France	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
77.66.20.217	Denmark	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	1
208.115.113.89	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/milum/templates/www.behazdaa.org.il	Block	1
148.251.67.18	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 148.251.67.18	Block	1
85.93.91.84	Germany	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.65.231	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
148.251.67.18	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for ww.aka.idf.il/giyus/main/	Block	1
95.108.158.171	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 95.108.158.171	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/english/news/jenin.stm)	Block	1
40.77.167.102	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
207.46.13.28	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/atal1/izkor/print_bottom.asp	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
81.89.96.89	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1