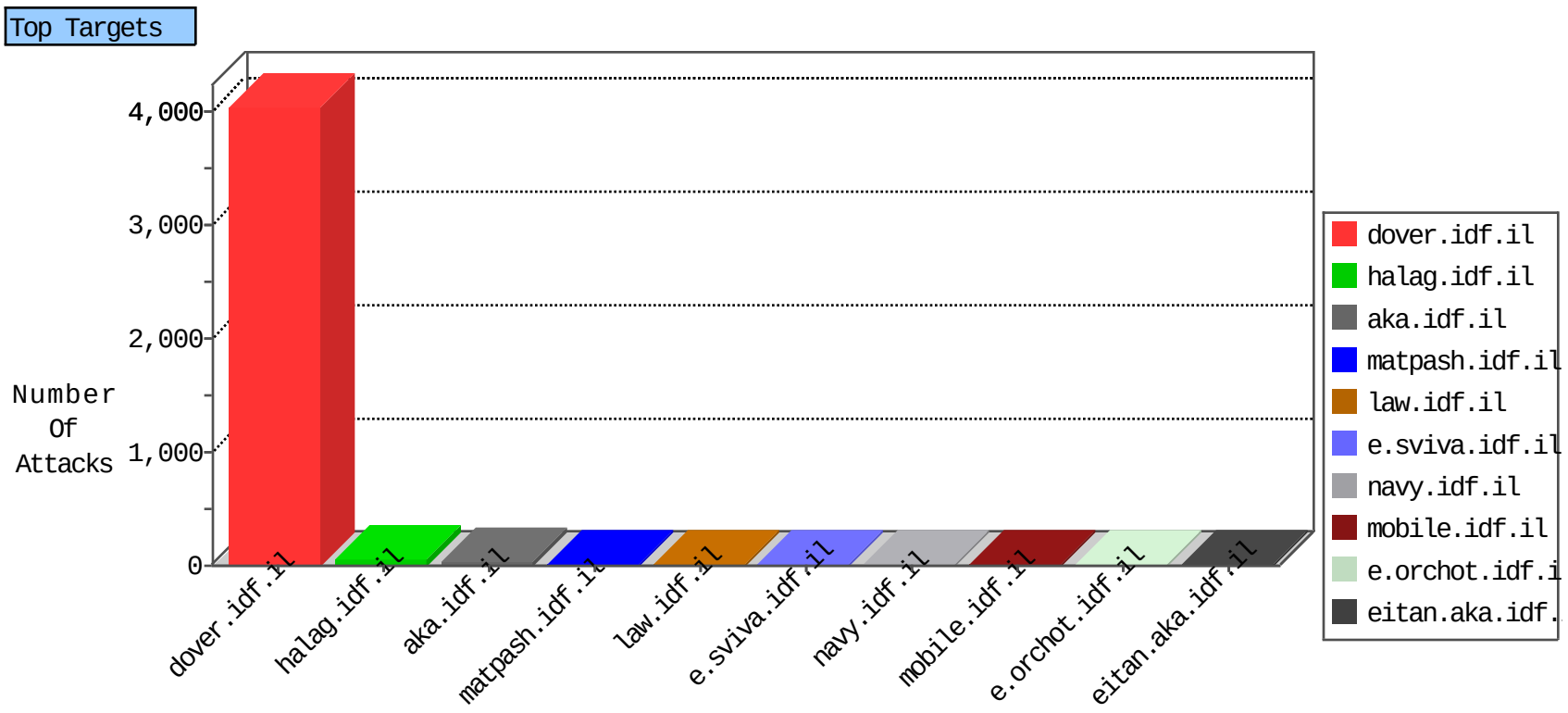
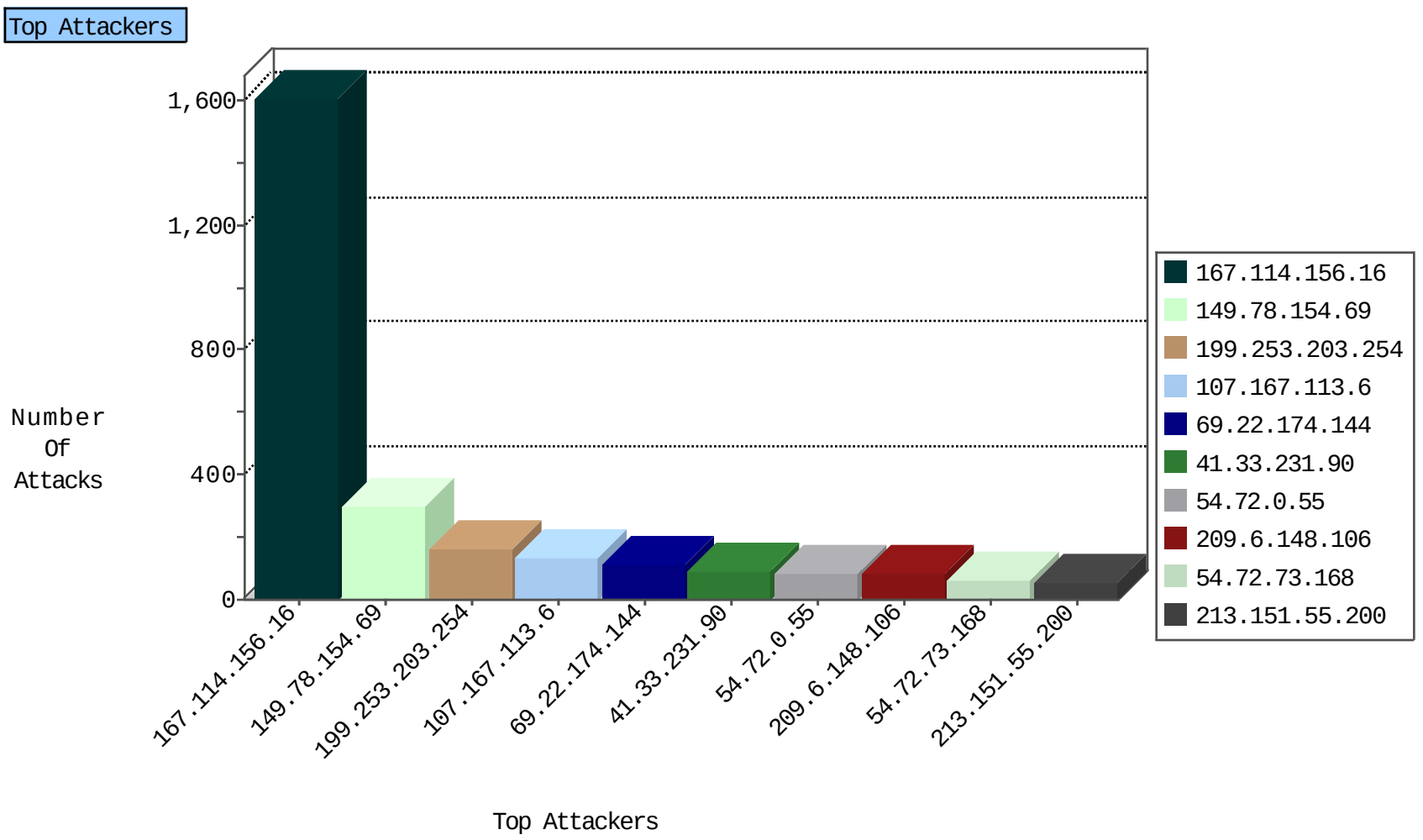
11-03-2015-03:04:03 to 11-03-2015-04:04:03

IDF Under Attack Daily Report





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

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	2866
66.249.64.181	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	184
185.32.179.131	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	34
104.60.173.253	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
223.4.244.13	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
180.210.201.106	Singapore	147.237.77.121	e.navy.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
71.6.216.57	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
82.102.169.210	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
5.8.66.69	Russian Federation	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1

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

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
187.122.224.78	Brazil	147.237.77.176	matpash.idf.il	16643: HTTP: Protected File Access (/proc/self/environ)	Block	1

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

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	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.67.13	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
223.4.244.13	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
223.4.244.13	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
1.235.195.234	147.237.76.196	Korea, Republic of	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
187.192.19.201	147.237.76.196	Mexico	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
187.192.19.201	147.237.76.196	Mexico	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
180.210.201.106	147.237.76.198	Singapore	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
180.210.201.106	147.237.0.34	Singapore	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
131.109.15.2	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 2048	1
223.4.244.13	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243	147.237.76.176		test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
223.4.244.13	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
217.12.202.110	147.237.0.34	Ukraine	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
1.235.195.234	147.237.76.196	Korea, Republic of	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
188.104.246.2	147.237.8.27	Germany	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
1.235.195.234	147.237.76.196	Korea, Republic of	e.sviva.idf.il	ET SCAN NMAP -f -sS	1
187.192.19.201	147.237.76.196	Mexico	e.sviva.idf.il	ET SCAN NMAP -sS window 2048	1
180.210.201.106	147.237.77.74	Singapore	law.idf.il	ET SCAN Potential SSH Scan	1
180.210.201.106	147.237.76.30	Singapore	himush.idf.il	ET SCAN Potential SSH Scan	1
131.109.15.2	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 4096	1
223.4.244.13	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
131.109.15.2	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -f -sS	1

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

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	294
199.253.203.254	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	160
107.167.113.6	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	135
69.22.174.144	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	112
54.72.0.55	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	84
209.6.148.106	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	80
41.33.231.90	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	79
54.72.73.168	Ireland	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	62
213.151.55.200	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	53
212.199.182.150	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	52
79.177.181.125	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	49
172.56.23.255	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	44
185.86.143.184		147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
52.16.5.197	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	38
99.127.169.246	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	37
218.214.148.224	Australia	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	36
119.224.26.199	New Zealand	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	32
24.233.180.97	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	31
212.179.90.106	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
74.64.124.39	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	28
50.87.144.145	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
207.46.13.95	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	26
37.142.68.51	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	25
82.80.25.221	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
68.180.228.112	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	24
66.249.64.139	United States	147.237.77.234	halag.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	22
66.249.64.250	United States	147.237.77.234	halag.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
66.249.78.166	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
173.14.73.66	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	19
66.249.78.159	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
185.32.179.131	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
151.80.31.112	Italy	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	17
2.54.33.210	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
109.200.30.154	United Kingdom	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	16
108.59.253.71	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
66.249.64.133	United States	147.237.77.234	halag.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
157.55.39.236	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
172.56.40.172	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	14
207.46.13.122	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
40.77.167.59	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
24.47.56.203	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
162.243.69.172	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	13
66.249.78.173	United States	147.237.77.216	dover.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.102.49	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
70.48.190.17	Canada	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
139.162.216.112	Netherlands	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	12
79.176.109.227	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
66.249.78.173	Israel	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11
141.209.151.191	United States	147.237.77.216	dover.idf.i	drop	First packet isn't SYN	drop	11

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

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
201.228.207.160	Colombia	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	3
208.115.111.73	United States	147.237.76.147	chinuch.aka.idf.i	Distributed Suspicious Response Code_Custom_Temporary	Block	2
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/3369.jpg	Block	1
77.56.26.69	Switzerland	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
66.249.67.34	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/7/112387.pdf	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1153-14220-he/dover.aspx	Block	1
66.249.65.251	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/articles.aspx	Block	1
77.56.26.69	Switzerland	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 77.56.26.69	Block	1
66.249.67.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/8/71558.pdf	Block	1
207.46.13.78	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training/catalog.asp	Block	1
66.249.67.12	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
84.229.249.4	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/request.aspx	None	1
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-he/cogat.aspx	Block	1
66.249.67.13	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
85.64.205.157	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
37.142.204.223	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.230.244	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/robots.txt	Block	1
66.249.67.26	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
85.250.211.174	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/giyus/miyun/miyunprocessquestionnaire.aspx	None	1

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