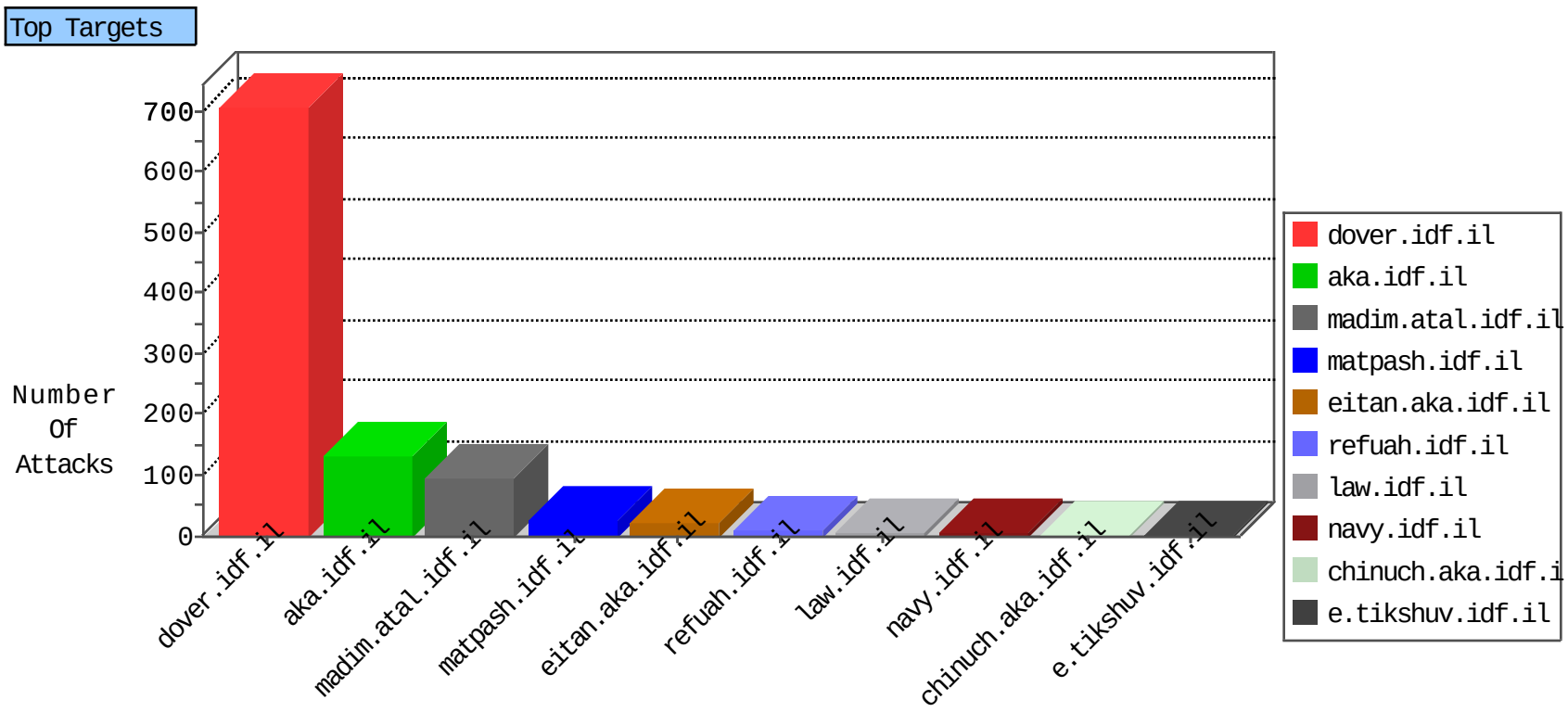
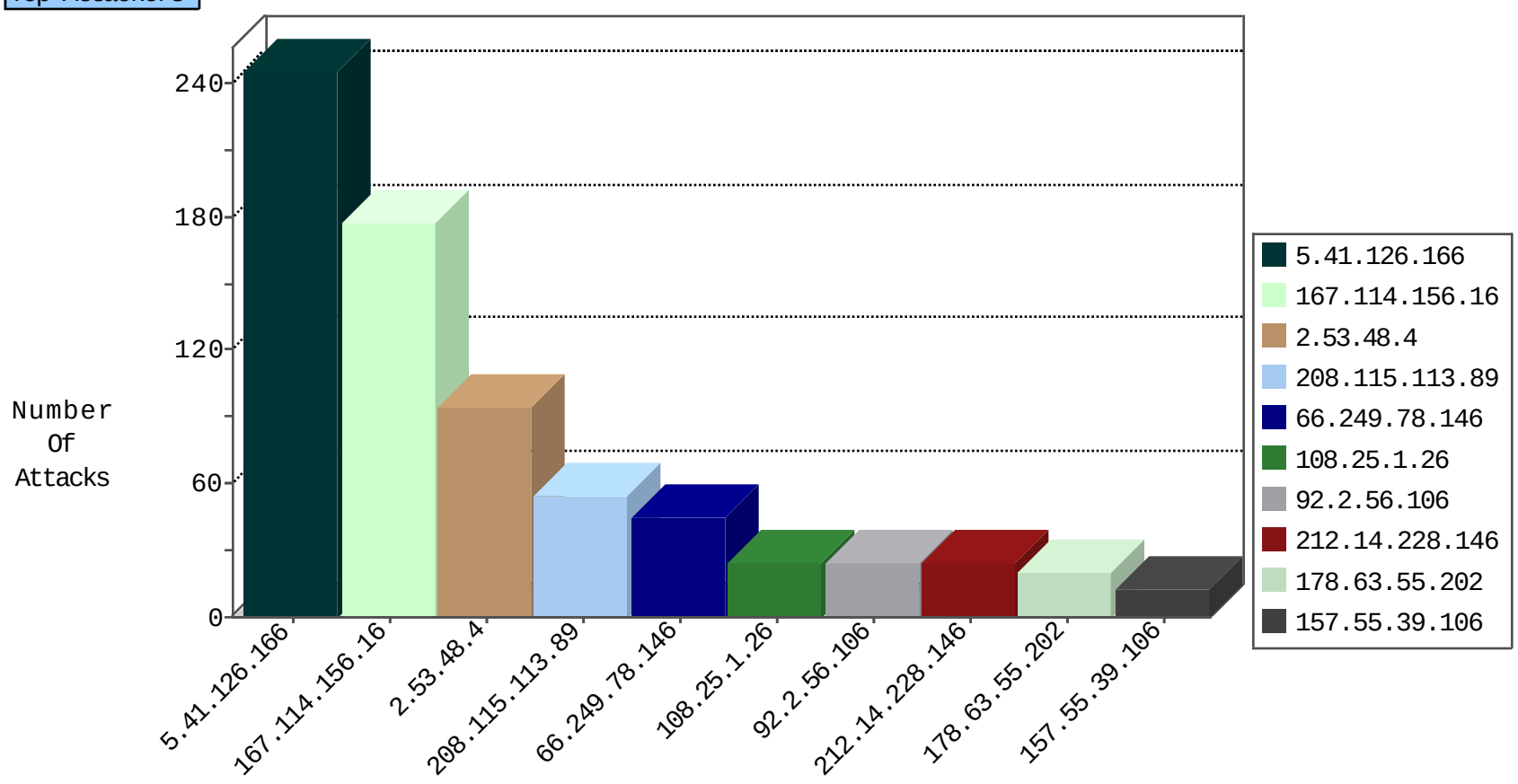
05-05-2016-01:08:08 to 05-05-2016-02:08:08

IDF Under Attack
Daily Report

Top Targets



Top Attackers



05-05-2016-01:08:08 to 05-05-2016-02:08:08

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	HTTP-POST-Segmented-DoS	dest-reset	7222
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	398
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
191.96.249.50	Chile	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1

05-05-2016-01:08:08 to 05-05-2016-02:08:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

05-05-2016-01:08:08 to 05-05-2016-02:08:08

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
94.102.48.195	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
66.240.213.93	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1
46.228.207.18	147.237.76.176	Germany	test.ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.228.207.18	147.237.0.33	Germany	idf.il	ET SCAN Potential VNC Scan 5900-5920	1
221.226.31.210	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -f -sS	1
46.228.207.18	147.237.0.16	Germany	my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
221.6.32.82	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -f -sS	1
187.188.72.11	147.237.76.38	Mexico	e.e.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
112.169.84.95	147.237.76.177	Korea, Republic of	ncore.idf.il	ET SCAN Potential SSH Scan	1
112.169.84.95	147.237.76.39	Korea, Republic of	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
66.240.213.93	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
46.228.207.18	147.237.76.198	Germany	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.228.207.18	147.237.0.34	Germany	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
221.226.31.210	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 2048	1
46.228.207.18	147.237.0.17	Germany	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
221.6.32.82	147.237.77.216	China	dover.idf.il	ET SCAN NMAP -sS window 2048	1
46.228.207.18	147.237.0.15	Germany	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
159.203.170.100	147.237.76.197	United States	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
112.169.84.95	147.237.76.42	Korea, Republic of	refuah.idf.il	ET SCAN Potential SSH Scan	1

05-05-2016-01:08:08 to 05-05-2016-02:08:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	51
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
5.41.126.166	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
108.25.1.26	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
178.63.55.202	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
92.2.56.106	United Kingdom	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
176.13.15.158	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
162.243.118.199	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
92.2.56.106	United Kingdom	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
157.55.39.106	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
212.14.228.146	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
79.183.212.129	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
149.202.73.13	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
87.211.107.246	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
84.95.208.20	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
87.70.11.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
87.71.14.168	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
207.46.13.22	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
207.46.13.178	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.14.228.146	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
212.14.228.146	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
104.132.1.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
176.228.137.171	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
157.55.39.134	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.53.180.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.250	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
66.249.78.254	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.111.23.1	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
72.80.142.83	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
66.249.93.180	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.148.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.247	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.65.2	United States	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.115.184.150	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
83.130.255.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
64.236.82.11	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
5.41.126.166	Saudi Arabia	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	2

05-05-2016-01:08:08 to 05-05-2016-02:08:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.41.126.166	Saudi Arabia	147.237.77.216	dover.idf.il	Multiple Malformed URL from 5.41.126.166	Block	99
5.41.126.166	Saudi Arabia	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 5.41.126.166	Block	99
2.53.48.4	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	94
5.41.126.166	Saudi Arabia	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 5.41.126.166	Block	10
66.249.78.147	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	3
157.55.39.134	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
54.186.53.55	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	2
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/3369.jpg	Block	1
17.142.156.103	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
213.151.36.128	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
85.250.146.74	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/1/	Block	1
54.186.53.55	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
2.53.180.72	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/3272.jpg	Block	1
37.47.66.193	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en	Block	1
141.212.122.145	United States	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to 147.237.76.147/	Block	1
54.186.53.55	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/wp-login.php	Block	1
164.132.161.38	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/born2.htm	Block	1
66.249.93.98	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
54.186.53.55	United States	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 54.186.53.55	Block	1
141.212.122.145	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.64.181	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/540-he/patzar/aspx	Block	1
167.61.98.168	Uruguay	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
66.249.93.110	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
157.55.2.139	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
167.61.98.168	Uruguay	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/wp-login.php	Block	1
85.250.146.74	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	1
54.186.53.55	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/wp-login.php	Block	1
157.55.39.106	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

05-05-2016-01:08:08 to 05-05-2016-02:08:08