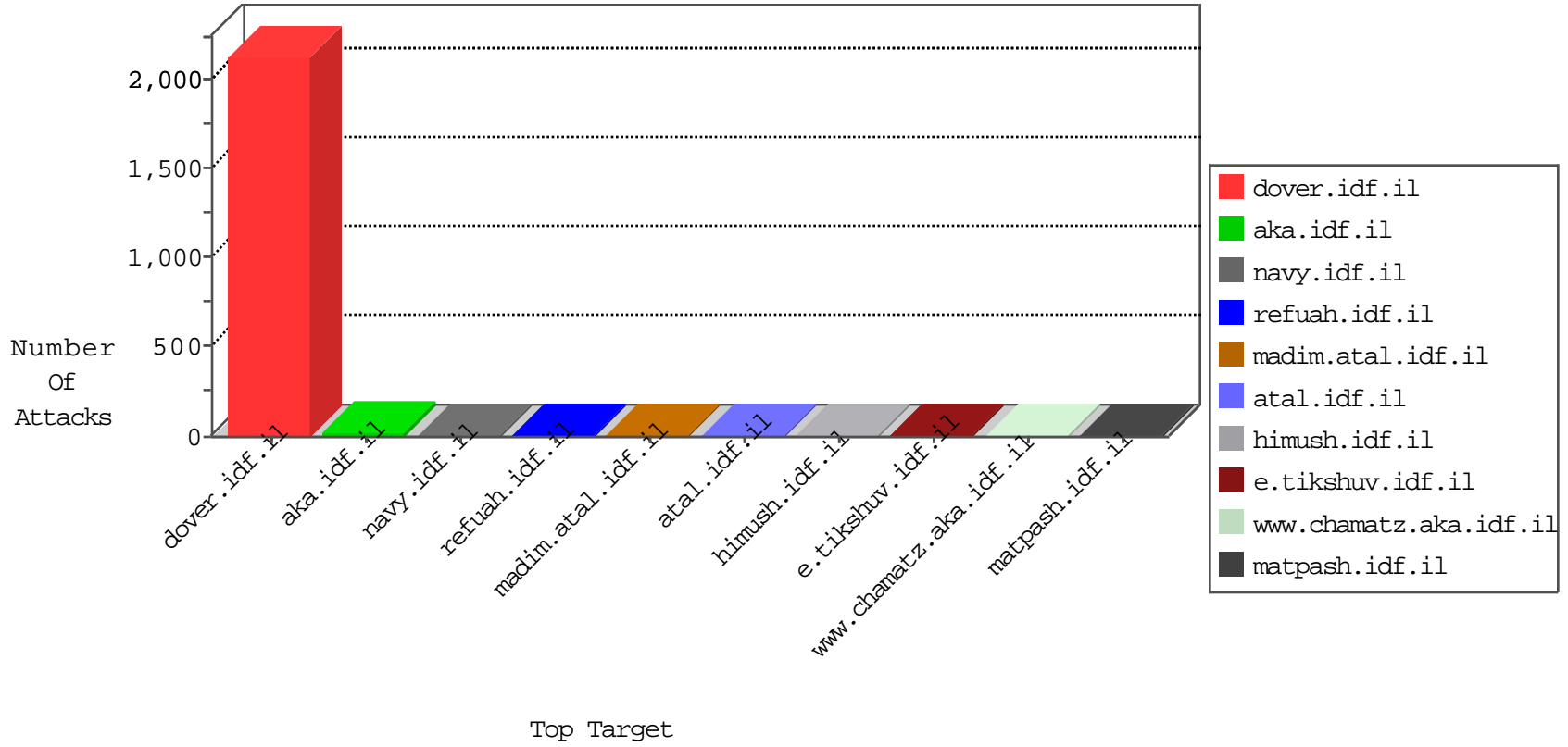


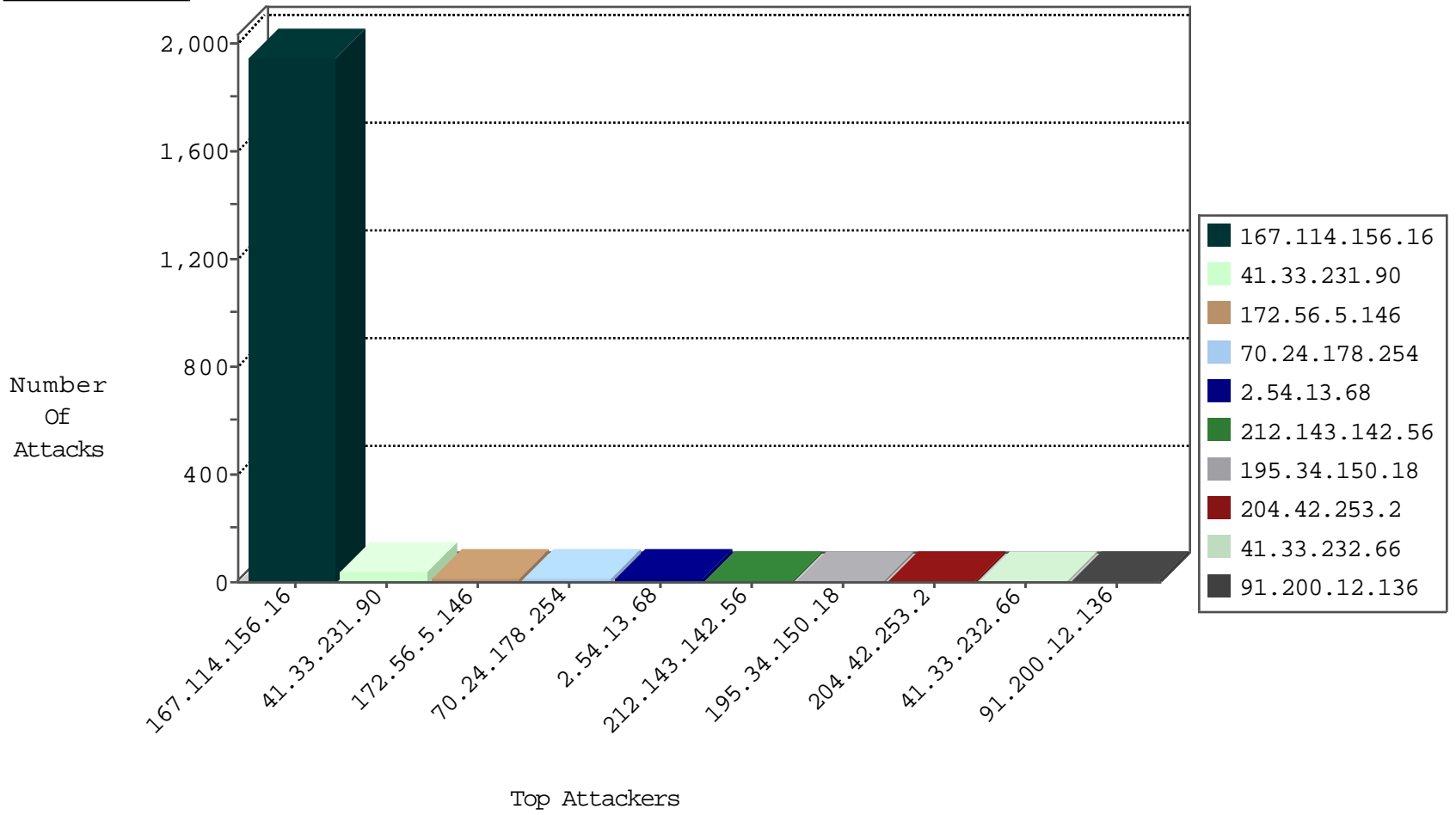
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3454
204.42.253.2	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	2
115.239.228.10	China	147.237.0.34	tikshuv.idf.il	Frk_Under_Attack_Con_Http	drop	2
204.42.253.2	United States	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	2
115.239.228.10	China	147.237.0.34	tikshuv.idf.il	Frk_Purple_Con_Limit_Http	drop	1
66.249.78.2	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	1
71.6.165.200	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
71.6.165.200	United States	147.237.76.148	ggcenter.aka.idf.il	Block_Udp_All_Nets	drop	1

12-25-2015-03:04:03 to 12-25-2015-04:04:03

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
66.249.66.9	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
27.199.9.156	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
112.33.3.69	147.237.8.46	China	e.chimuch.idf.il	ET SCAN Potential SSH Scan	1
112.33.3.69	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
112.33.3.69	147.237.8.14	China	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
87.197.159.157	147.237.0.15	Slovakia	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
46.161.40.120	147.237.76.198	Russian Federation	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
218.104.49.211	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
114.96.166.154	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
112.33.3.69	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
112.33.3.69	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.181	147.237.77.234	Netherlands	halag.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
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
172.56.5.146	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
70.24.178.254	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
2.54.13.68	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
91.200.12.136	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
188.166.218.89	Russian Federation	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
66.249.64.163	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
37.26.147.245	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
195.154.226.90	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
84.109.90.9	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.136.37	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
149.78.106.204	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
133.130.58.99	Japan	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
91.200.12.7	Ukraine	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
91.200.12.7	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
68.180.228.112	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
54.241.198.78	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
66.249.64.169	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
141.212.122.139	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
65.55.218.33	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.68	United States	147.237.77.61	e.cogat.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
23.29.122.195	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
149.78.106.204	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
67.227.163.231	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
141.212.122.132	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
131.253.26.251	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
198.27.82.182	Canada	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
85.25.103.119	Germany	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
178.32.53.53	United Kingdom	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
71.6.165.200	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.140	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
66.230.230.230	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
141.212.122.69	United States	147.237.77.61	e.cogat.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
23.96.208.137	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
93.115.95.201	Anonymous Proxy	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
193.90.12.86	Norway	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
81.7.16.13	Germany	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
68.3.86.103	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.138	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
199.87.154.255	Canada	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
2.54.174.172	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
178.32.53.94	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.6	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.140	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.13.60	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	5
46.121.104.234	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
158.69.52.102	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
37.142.68.8	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
213.8.204.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.10.52	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
149.202.74.134	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
37.142.68.120	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/xmlrpc.php	Block	1
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/3/size220x0/16833.jpg	Block	1
109.201.154.241	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
54.186.248.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
2.54.158.226	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
216.163.188.223	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1934-he/cogat.aspx	Block	1
37.187.129.166	France	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/clientscripts/jquery/jquery-1.4.2.min.js	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
141.212.122.129	United States	147.237.77.74	law.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
66.249.66.131	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/6/size100x0/3156.jpg	Block	1
5.79.242.126	Russian Federation	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
158.69.52.102	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 158.69.52.102	Block	1
93.115.95.202	Anonymous Proxy	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.19.86.177	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
141.212.122.129	United States	147.237.77.170	maarachot.idf.il	Malformed URL proxytest.zmap.io:80	Block	1
66.249.66.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/size100x0/3238.jpg	Block	1
158.69.52.102	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	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
66.249.66.191	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/2317.png	Block	1
37.142.68.120	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.166.186.226	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
216.38.216.197	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1