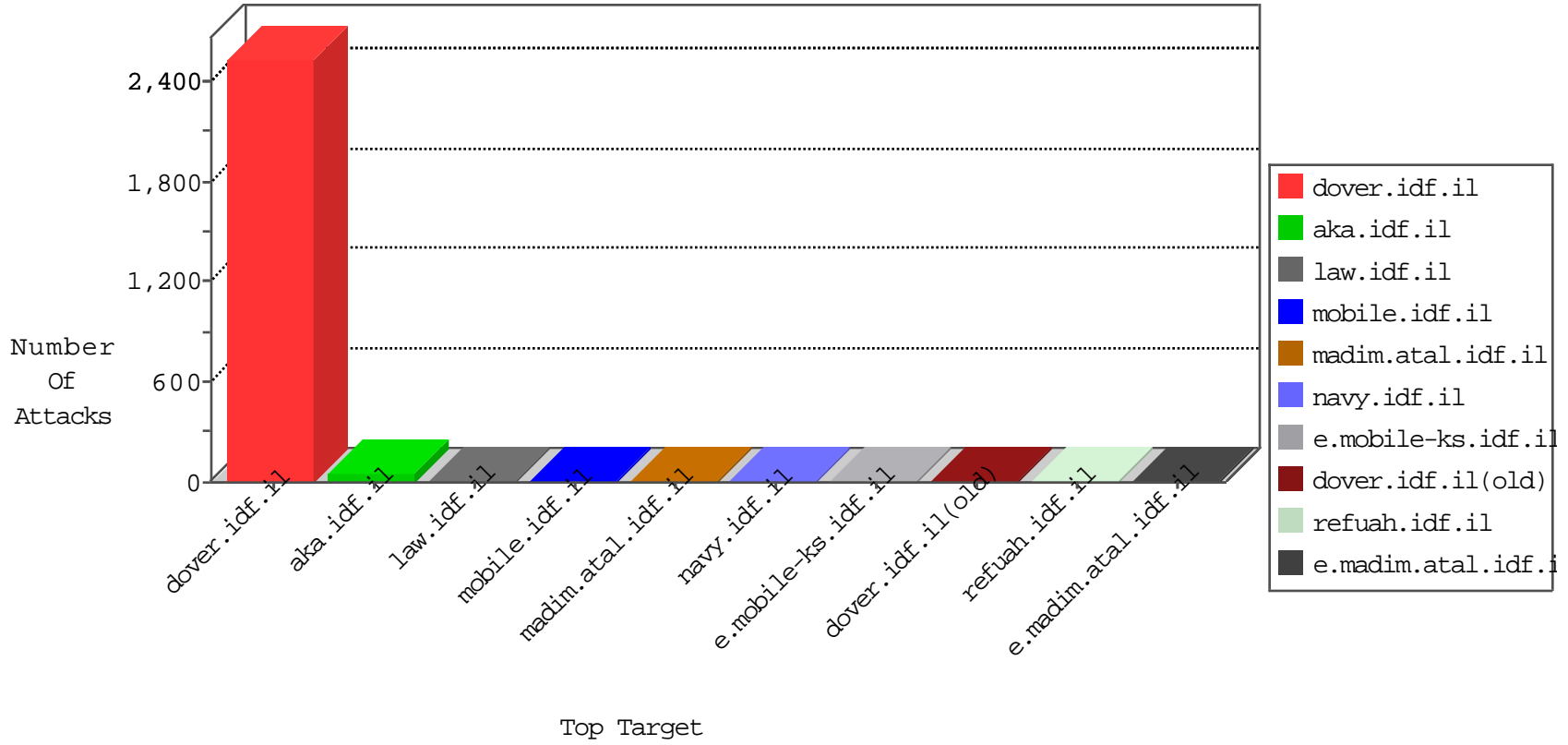


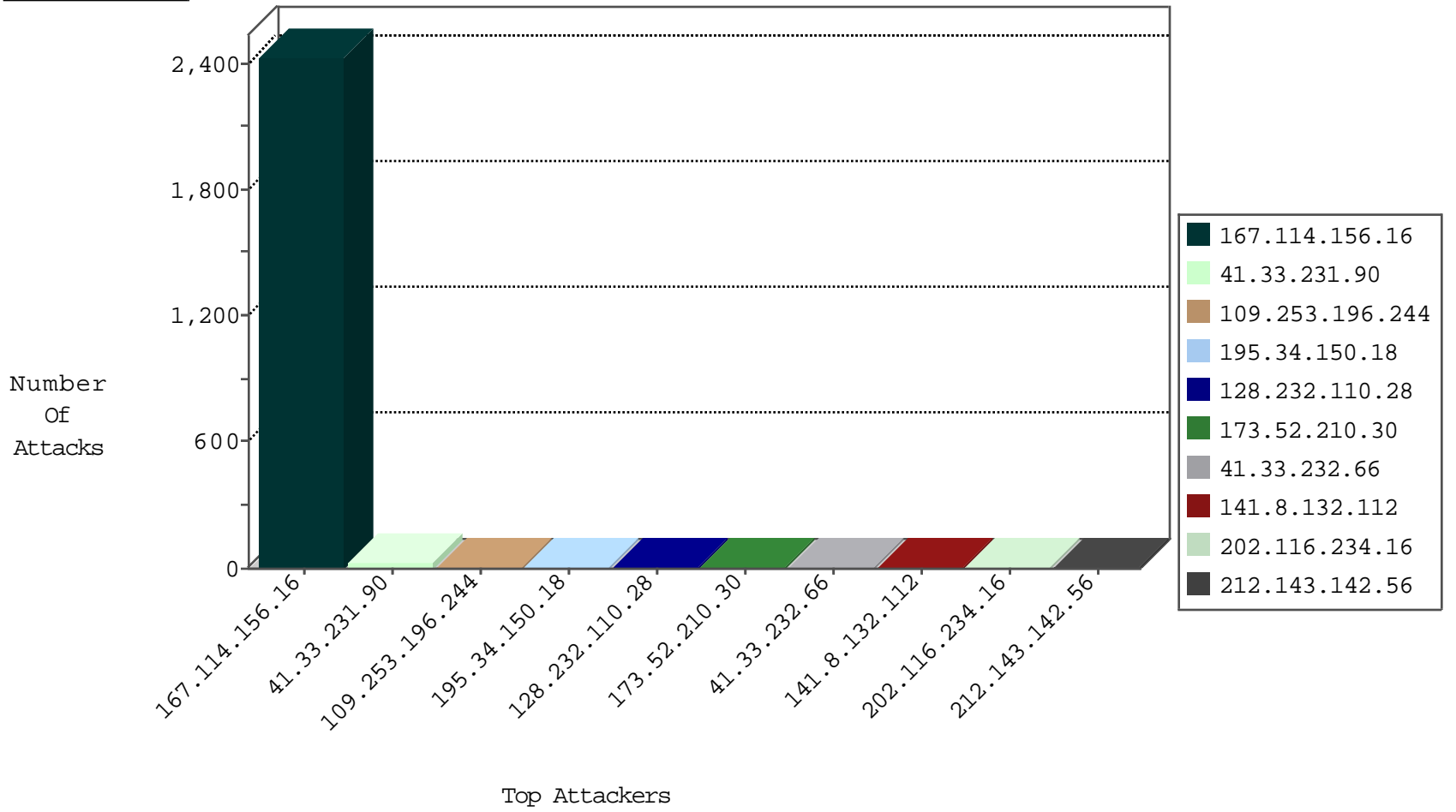
# IDF Under Attack Daily Report



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	3062
78.170.0.184	Turkey	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
89.248.160.138	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
89.248.160.138	Netherlands	147.237.76.148	ggcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
78.170.0.184	Turkey	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.225.121	France	147.237.72.166	aka.idf.il	0543: HTTP: php.cgi Access	Block	1
23.91.70.77	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1

## 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	11
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
23.91.70.77	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	3
131.109.15.15	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 2048	1
199.191.56.188	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 3072	1
131.109.15.15	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 4096	1
131.109.15.15	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -f -sS	1
199.191.56.188	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 4096	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	Block HTTP Non Compliant	Failed to handle connection data	monitor	11
109.253.196.244	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
173.52.210.30	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.130.227.133	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
157.55.39.20	United States	147.237.72.166	aka.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
109.67.216.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.210.121	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
157.55.39.211	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.175.193.232	Germany	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
2.54.16.95	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
128.232.110.28	United Kingdom	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
128.232.110.28	United Kingdom	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
204.79.180.181	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
141.212.121.192	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
208.115.113.89	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
128.232.110.28	United Kingdom	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
188.138.61.79	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
202.116.234.16	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.17.184.228	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
46.183.222.166	Latvia	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
216.218.206.102	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.79.68.161	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
204.11.50.131	Canada	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
94.242.246.24	Luxembourg	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
193.90.12.90	Norway	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
74.82.47.54	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.121.192	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
202.116.234.16	China	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.10.210.199	Germany	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
185.60.144.33	Switzerland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.104	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
104.130.78.65	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
193.171.202.150	Austria	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
74.82.47.54	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.199	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.121.192	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
115.230.124.164	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
202.116.234.16	China	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
85.93.218.204	Luxembourg	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
185.65.135.227	Sweden	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
74.82.47.31	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
158.69.201.128	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.213.244	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
157.55.39.250	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.250	Block	2
46.121.106.142	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
204.13.201.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.241.192.41	Germany	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
46.19.86.127	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
94.102.153.58	United Kingdom	147.237.72.167	ishurim.aka.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	None	1
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/templatecontrols/generic/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
94.102.153.58	United Kingdom	147.237.72.167	ishurim.aka.idf.il	Multiple signatures from 94.102.153.58	Block	1
66.249.78.216	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.78.216	Block	1
188.165.225.121	France	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 188.165.225.121	Block	1
68.180.229.47	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
65.132.59.34	United States	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 65.132.59.34 (sigalgs DoS Attack)	None	1
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	1
66.249.78.216	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1778	Block	1
37.187.43.27	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
188.165.225.121	France	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/cgi-bin/php-cgi	Block	1
68.180.231.40	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/228-he/faq.aspx	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/	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
66.249.78.230	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1779	Block	1
40.77.167.102	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/faq.aspx	None	1