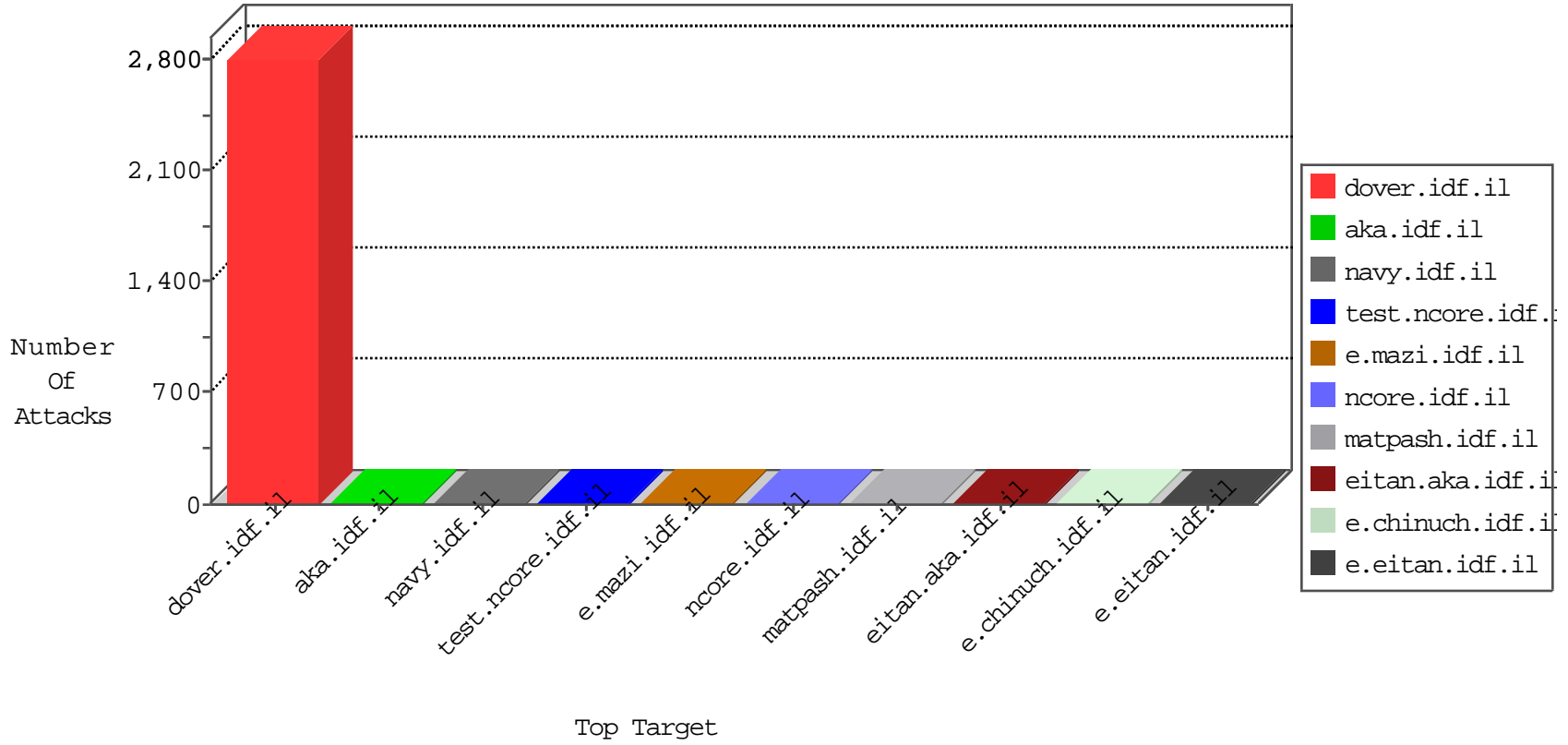


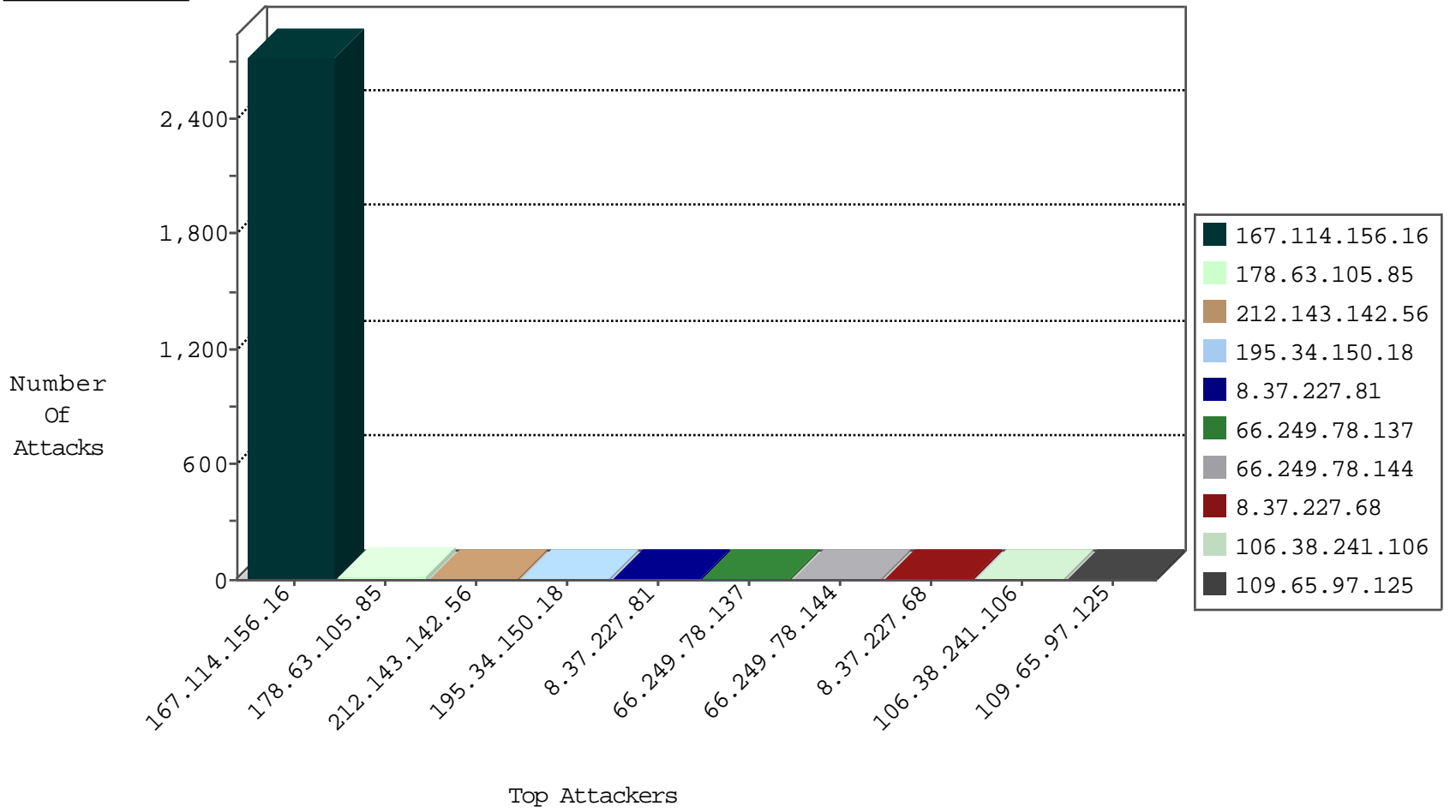
# IDF Under Attack Daily Report



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	3689
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
182.140.167.188	China	147.237.8.24	e.lifestyle.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.88	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.116	United States	147.237.77.233	atal.idf.il	Block_Ntp_All_Net	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	2
46.116.11.31	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
134.249.53.96	Ukraine	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Block	1

## 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
104.232.98.38	147.237.0.16		my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
47.23.96.141	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
46.132.187.214	147.237.77.216	Finland	dover.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.76.197	China	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
104.232.98.38	147.237.0.16		my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
47.23.96.141	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 4096	1
46.132.187.214	147.237.77.234	Finland	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	23
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
178.63.105.85	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	4
178.63.105.85	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	4
8.37.227.68	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	4
66.249.78.137	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.78.144	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
8.37.227.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	4
109.65.97.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	3
178.63.105.85	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	3
178.63.105.85	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	3
8.37.227.69	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	3
178.63.105.85	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	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
66.249.78.130	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.9.164.175	Norway	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
79.178.135.160	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
207.46.13.21	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
178.63.105.85	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	2
74.82.47.11	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.209	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.168	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.26.147.208	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.165	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.23	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.209	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
178.63.105.85	Germany	147.237.76.39	mobile.meitav.idf.i	drop	SAM rule	drop	1
141.212.122.168	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.155	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
71.6.165.200	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.126	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
38.229.1.15	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.166	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.36	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
159.226.95.66	China	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.156	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
72.9.148.10	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
141.212.122.167	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.157	United States	147.237.76.148	ggcenter.aka.idf.il	drop		drop	1
74.82.47.11	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.118	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
178.63.105.85	Germany	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
141.212.122.167	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.38.241.106	China	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.158	United States	147.237.76.148	ggcenter.aka.idf.il	drop		drop	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.102.7.226	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
2.54.10.44	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1432	Block	2
134.249.53.96	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-19163-he/dover.aspx	Block	1
207.46.13.21	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/	Block	1
74.208.12.240	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
37.48.118.96	Netherlands	147.237.77.216	dover.idf.il	Parameter Type Violation &l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
157.55.12.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
207.46.13.123	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
74.208.12.240	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.php	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
87.71.29.116	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
66.102.7.233	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/size100x0/2802.jpg	Block	1
5.28.191.224	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
134.249.53.96	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.78.45	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/departmentslobby/departmentslobby.aspx	Block	1
197.231.221.211	Liberia	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
68.180.230.43	United States	147.237.76.200	eitan.aka.idf.il	Unknown Parameter &SortDir in www.eitan.aka.idf.il/1103-he/eitan.aspx	None	1
5.28.191.224	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1