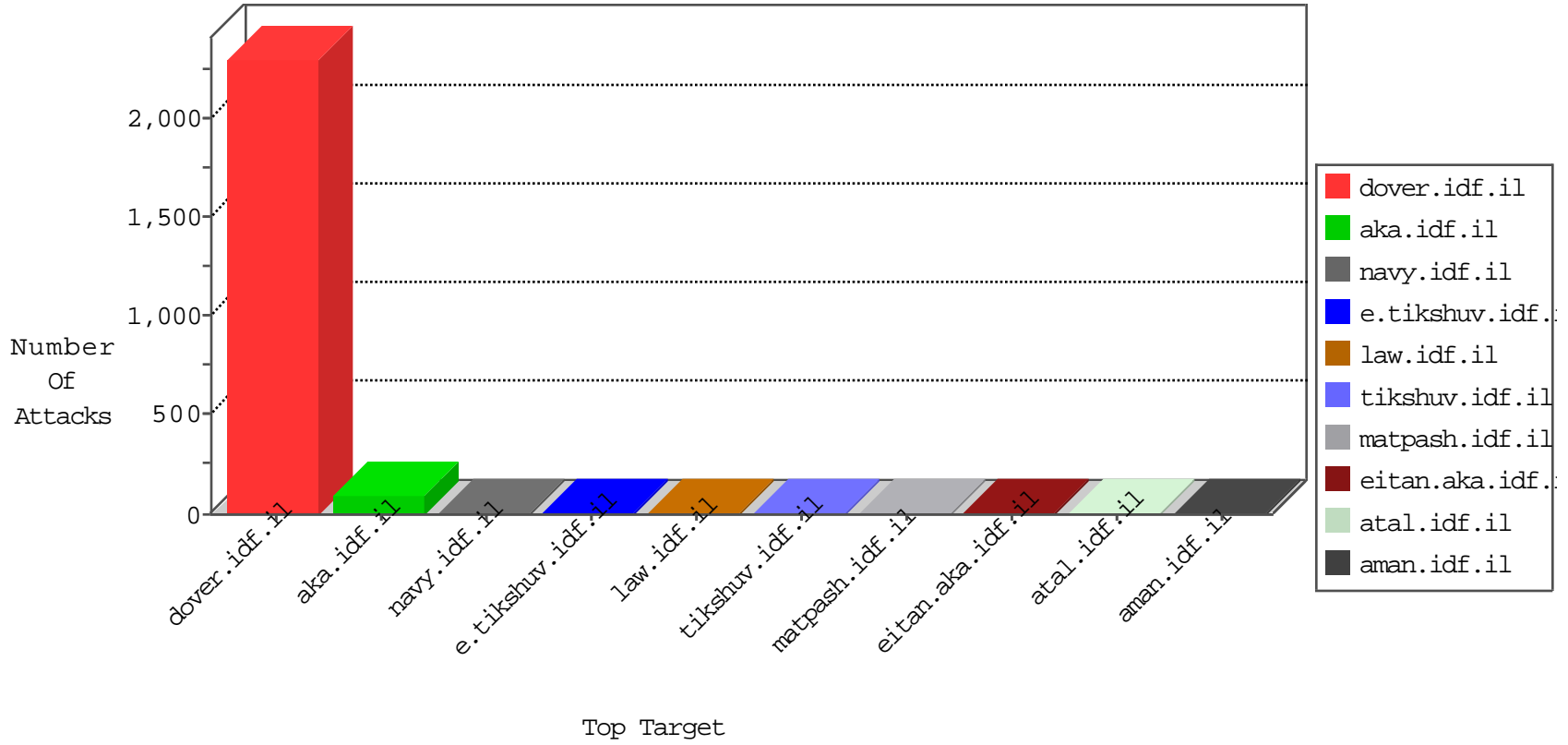


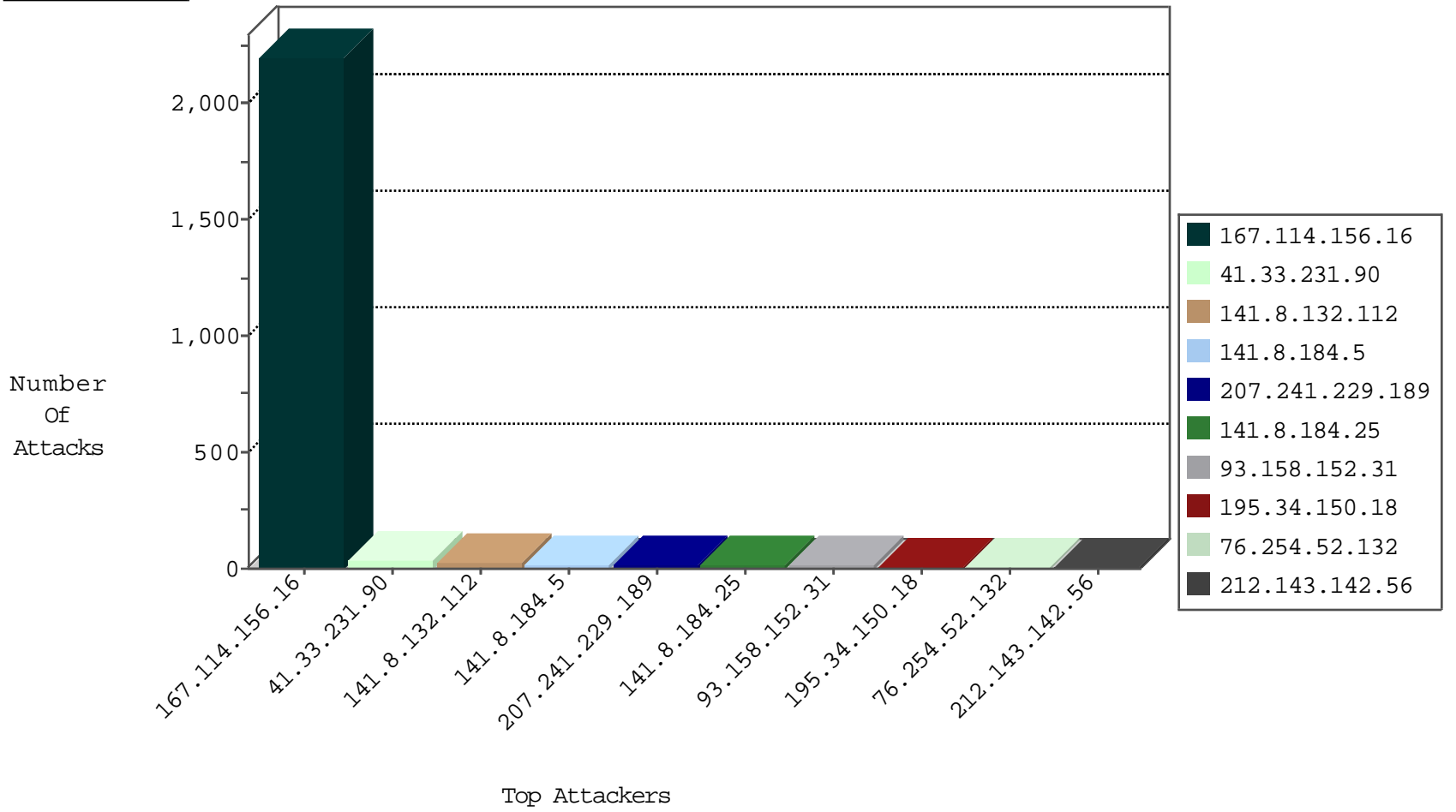
IDF Under Attack Daily Report



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	3003
184.26.161.65	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.137.81.122	Ireland	147.237.77.176	matpash.idf.il	5670: HTTP: SQL Injection (SELECT)	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
46.137.81.122	147.237.77.176	Ireland	matpash.idf.il	SQL Injection - Select From	3
66.249.74.93	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
172.98.200.237	147.237.76.147		chimuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
212.179.227.181	147.237.77.212	Israel	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
172.98.200.237	147.237.76.147		chimuch.aka.idf.il	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	drop	SAM rule	drop	36
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
141.8.184.5	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
141.8.184.25	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
207.241.229.189	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	15
93.158.152.31	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
216.249.107.200	United States	147.237.77.74	law.idf.il	drop	SAM rule	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
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.237.82.50	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
76.254.52.132	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
52.53.221.104	United States	147.237.8.50	e.tikshuv.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	2
157.55.39.22	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
40.77.167.50	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
77.77.76.3	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
157.55.39.147	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
76.254.52.132	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
207.46.13.108	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
52.53.218.177	United States	147.237.8.50	e.tikshuv.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	2
81.169.237.146	Germany	147.237.8.46	e.chinuch.idf.i	drop	SAM rule	drop	2
67.212.234.181	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
173.254.216.68	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
5.29.84.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.203	United States	147.237.8.50	e.tikshuv.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1
108.168.185.133	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.103	United States	147.237.0.35	akaws.idf.il	drop		drop	1
85.25.103.12	Germany	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
193.90.12.88	Norway	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
74.82.47.35	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.126.252.11	Romania	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
141.212.122.206	United States	147.237.76.198	e.yohalan.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.104	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
54.176.17.88	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
141.212.122.196	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.25.103.119	Germany	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
76.254.52.132	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
179.210.108.39	Brazil	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.207	United States	147.237.76.198	e.yohalan.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1
208.93.66.155	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
77.247.182.246	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
184.105.139.107	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
64.246.165.170	United States	147.237.72.166	aka.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.197	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
93.115.95.216	Anonymous Proxy	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.215.103	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	2
84.108.32.126	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.64.239	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
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
91.228.196.139	Poland	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.65.48	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/sachar/faq.aspx	Block	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
91.228.196.139	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-signup.php	Block	1
176.126.252.11	Romania	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
77.40.129.123	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
207.232.55.134	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
104.192.0.18	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.64.229	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1249-he/atal.aspx	Block	1
185.10.71.107	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
77.40.129.123	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
207.232.55.134	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.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
66.249.64.234	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1246-he/atal.aspx	Block	1
187.195.19.87	Mexico	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	Block	1