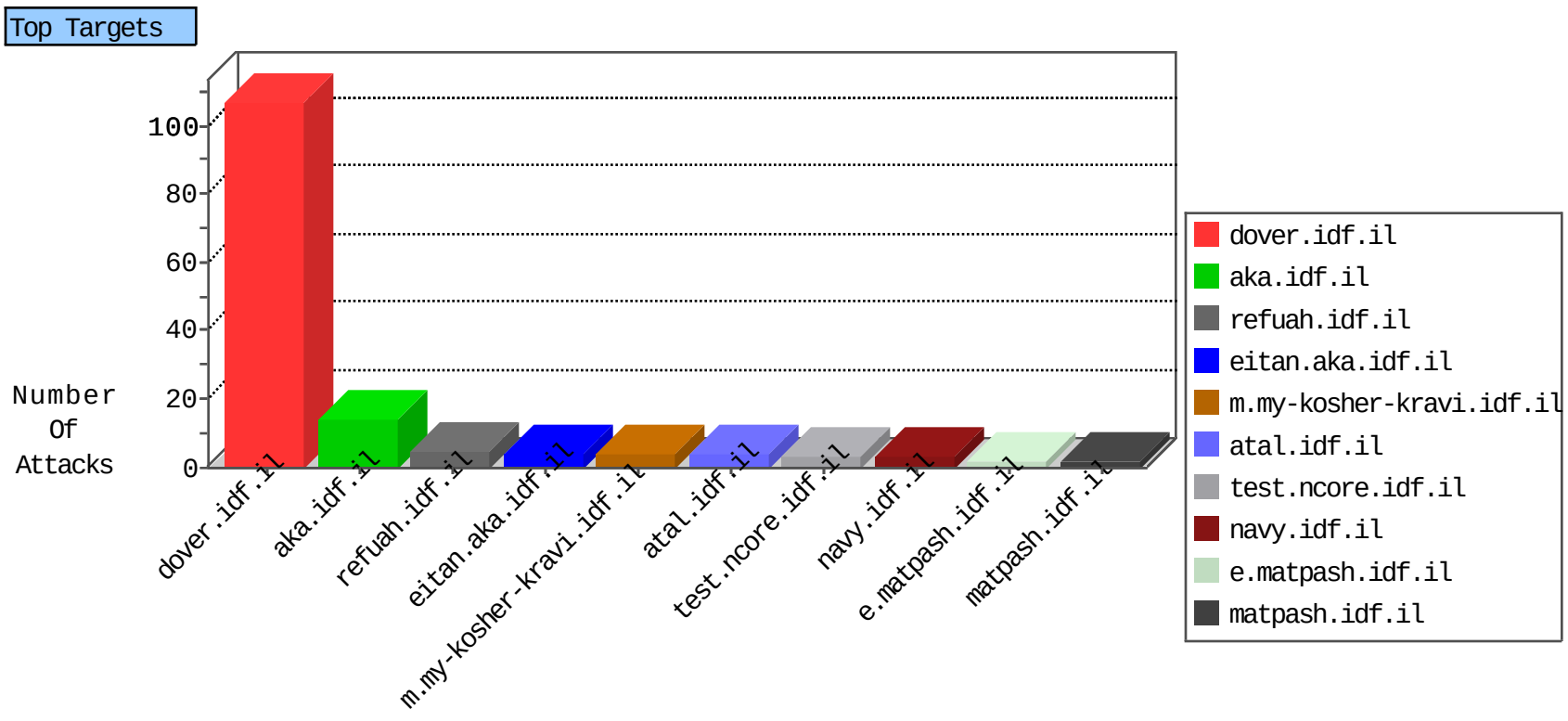
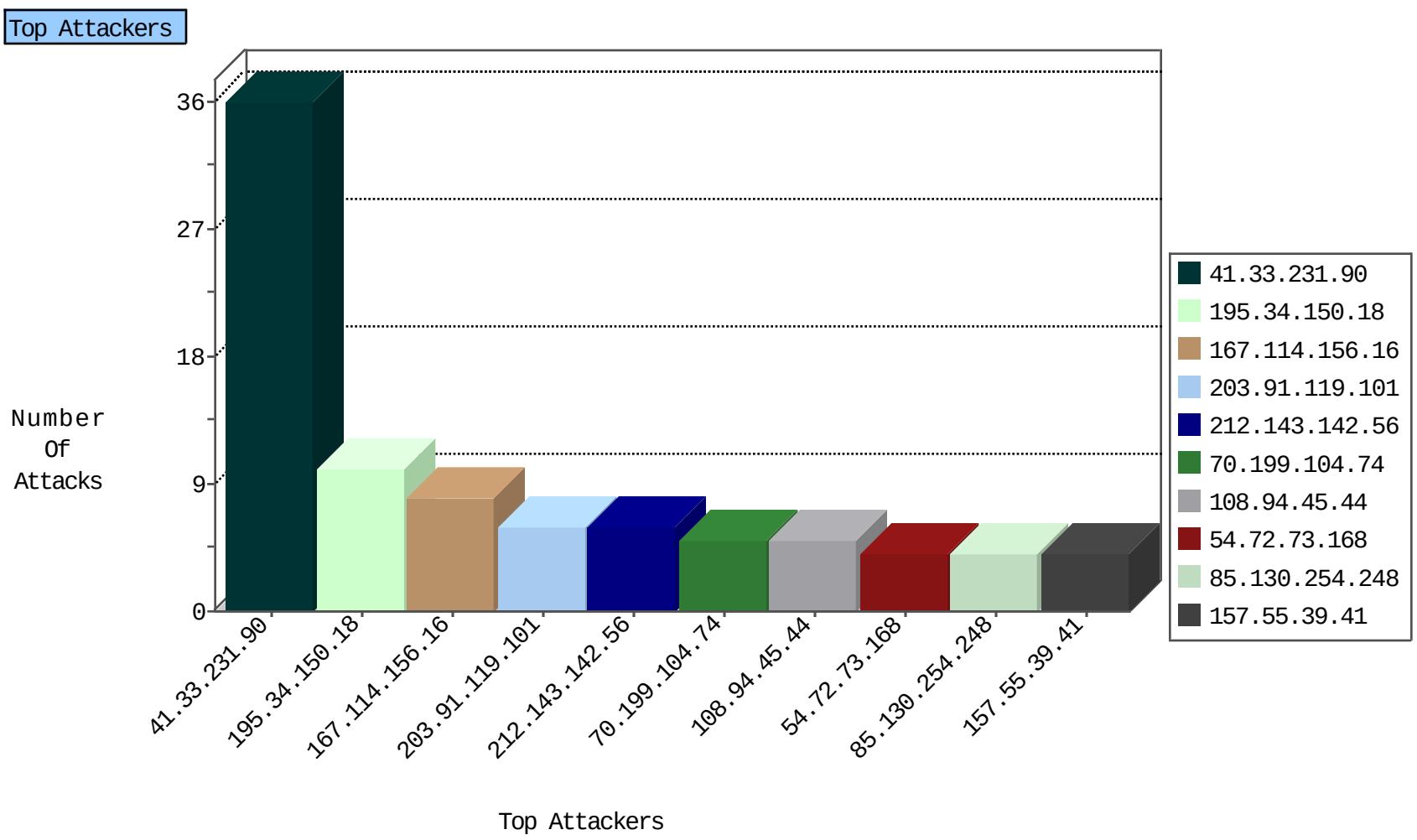
12-23-2015-04:04:04 to 12-23-2015-05:04:04

IDF Under Attack Daily Report





12-23-2015-04:04:04 to 12-23-2015-05:04:04

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	260
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
115.239.228.10	China	147.237.0.17	m.my-kosher-kravi.idf.il	Frk_Under_Attack_Con_Http	drop	2
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	F_Dover_Under_Attack_Con_Http	drop	2
115.239.228.10	China	147.237.0.17	m.my-kosher-kravi.idf.il	Frk_Purple_Con_Limit_Http	drop	1

12-23-2015-04:04:04 to 12-23-2015-05:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.147	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-23-2015-04:04:04 to 12-23-2015-05:04:04

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	5
75.145.81.98	147.237.77.178	United States	e.matpash.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
218.108.132.58	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.214	147.237.77.233		atal.idf.il	ET DOS SSL Bomb DoS Attempt	1
183.82.106.200	147.237.76.176	India	test.ncore.idf.il	ET SCAN NMAP -sS window 2048	1
180.153.104.125	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 3072	1
104.219.238.10	147.237.77.216		dover.idf.il	ET SCAN NMAP -sS window 1024	1
78.193.2.8	147.237.72.166	France	aka.idf.il	ET SCAN NMAP -sS window 1024	1
183.82.106.200	147.237.76.176	India	test.ncore.idf.il	ET SCAN NMAP -sS window 4096	1
183.82.106.200	147.237.76.176	India	test.ncore.idf.il	ET SCAN NMAP -f -sS	1
112.196.49.101	147.237.77.179	India	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
78.193.2.8	147.237.77.74	France	law.idf.il	ET SCAN NMAP -sS window 1024	1

12-23-2015-04:04:04 to 12-23-2015-05:04:04

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
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
157.55.39.41	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
70.199.104.74	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.130.254.248	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
2.54.19.16	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
185.130.5.214		147.237.77.233	atal.idf.il	SSL Enforcement Violation	TLS Servers Cipher Suites Vulnerability Scanning Tools	reject	2
157.55.39.79	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
85.130.254.248	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
141.212.122.171	United States	147.237.0.35	akaws.idf.il	drop		drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
176.58.245.111	Greece	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.161	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
77.77.76.3	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
2.54.19.16	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
216.218.206.76	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
141.212.122.172	United States	147.237.0.35	akaws.idf.il	drop		drop	1
101.198.159.31	China	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
58.215.220.78	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
184.105.139.110	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.161	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
77.77.76.3	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.76	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
109.2.242.6	France	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.162	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
84.108.121.108	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
137.116.71.170	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
70.199.104.74	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.162	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
173.54.44.94	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1

12-23-2015-04:04:04 to 12-23-2015-05:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
203.91.119.101	Mongolia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
203.91.119.101	Mongolia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	3
84.108.138.180	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	2
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/8/63578.doc	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
108.94.45.44	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in URL	Block	1
71.166.126.178	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
45.55.167.12		147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1313-en/cogat.aspx/timeout=3600	Block	1
183.13.153.240	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.79.75	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1385943851000	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
108.94.45.44	United States	147.237.76.42	refuah.idf.il	NULL Character in Method Â¬[[#0]][[#0]][[#0]]p;[[#23]]ÃœÂ‘ 0W'[[#31]]DÂ¹Â°ÃºÃªmCvÃ°ÂžFÂšÂ¸ AÂµÂŸÃ¿ÃªÂ²Â…/Ã¤Âš r_iÂ¡[[#2]]bRÂ˜IÃ¥Ã¼[[#30]]Â›KhvÃ—Â¥Ã“[[#6]]Â?Â°Ã·}[[#11]]Ã°Ã—Ã„ Ã?Â±	Block	1
74.82.47.2	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
46.166.190.138	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
191.252.48.178	Brazil	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/test/wp-admin/	Block	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
66.249.79.77	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/e	Block	1
208.113.155.20	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/wordpress/wp-admin/	Block	1
108.94.45.44	United States	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method Â¬[[#0]][[#0]][[#0]]p;[[#23]]ÃœÂ‘ 0W'[[#31]]DÂ¹Â°ÃºÃªmCvÃ°ÂžFÂšÂ¸ AÂµÂŸÃ¿ÃªÂ²Â…/Ã¤Âš r_iÂ¡[[#2]]bRÂ˜IÃ¥Ã¼[[#30]]Â›KhvÃ—Â¥Ã“[[#6]]Â?Â°Ã·}[[#11]]Ã°Ã—Ã„ Ã?Â±	Block	1
66.249.64.224	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
108.94.45.44	United States	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	1
66.249.79.79	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1385943851000	Block	1
216.18.193.134	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
141.212.122.80	United States	147.237.0.15	kosher-kravi.idf.il	Multiple Malformed URL from 141.212.122.80	Block	1
91.231.192.149	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
66.249.78.111	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
108.94.45.44	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Method Â¬[[#0]][[#0]][[#0]]p;[[#23]]ÃœÂ‘ 0W'[[#31]]DÂ¹Â°ÃºÃªmCvÃ°ÂžFÂšÂ¸ AÂµÂŸÃ¿ÃªÂ²Â…/Ã¤Âš r_iÂ¡[[#2]]bRÂ˜IÃ¥Ã¼[[#30]]Â›KhvÃ—Â¥Ã“[[#6]]Â?Â°Ã·}[[#11]]Ã°Ã—Ã„ Ã?Â±	Block	1
66.249.79.119	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
216.18.193.134	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
141.212.122.80	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Malformed URL from 141.212.122.80	Block	1
107.150.56.90	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/wp-admin/	Block	1

12-23-2015-04:04:04 to 12-23-2015-05:04:04