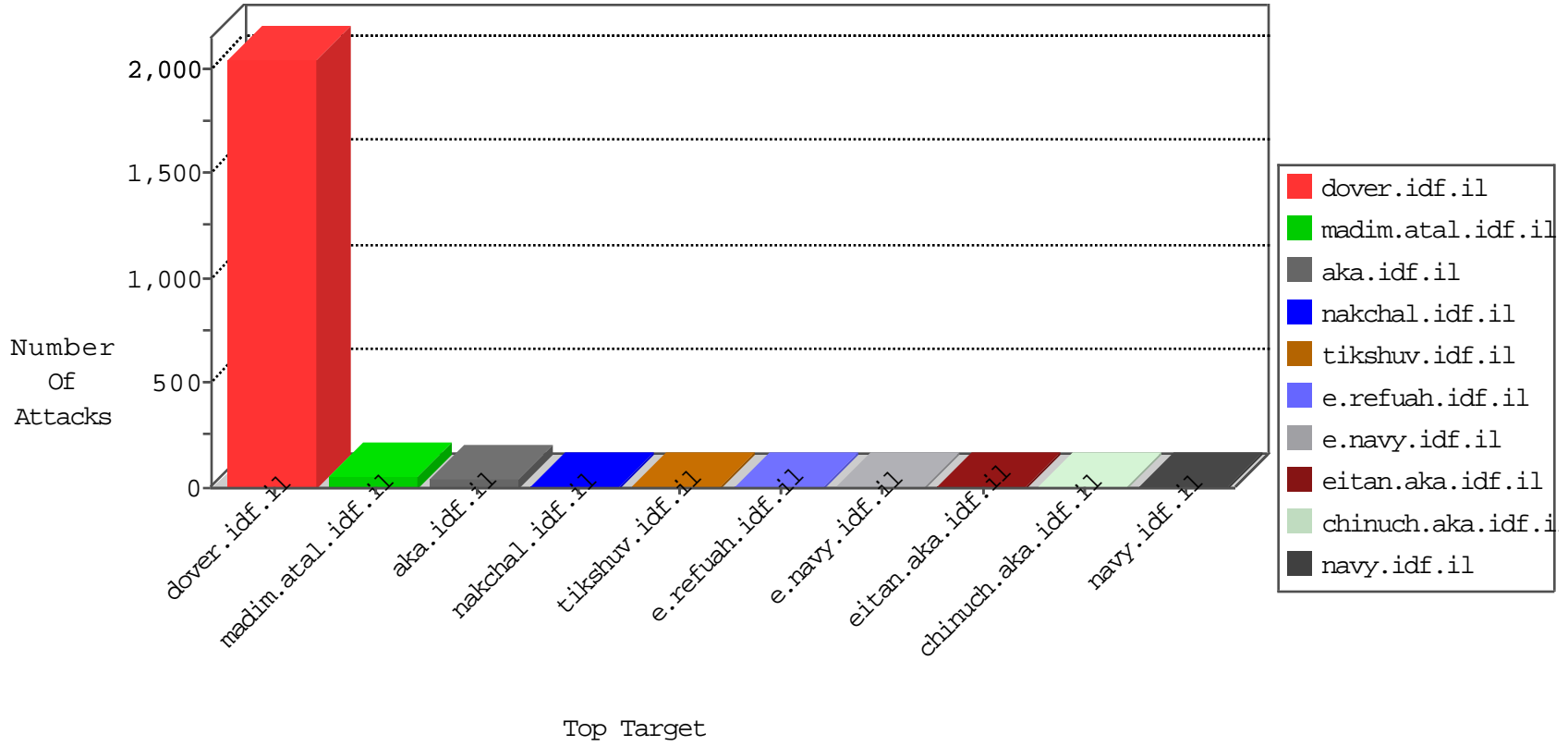


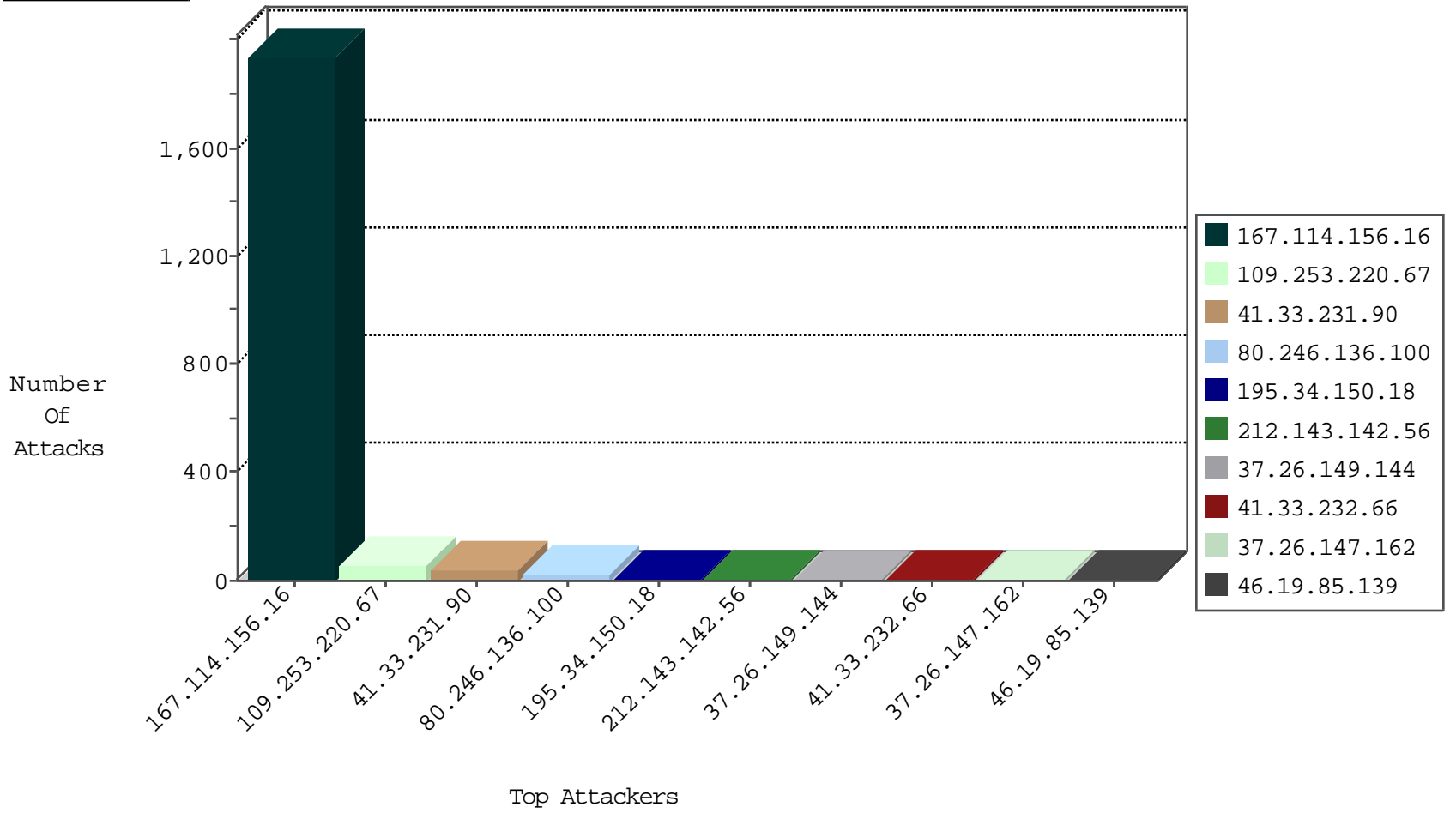
IDF Under Attack Daily Report



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	3140
204.42.253.2	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1
77.247.178.132	Netherlands	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
172.98.67.67		147.237.76.198	e.yohanan.idf.il	Block_Ntp_All_Net	drop	1

12-25-2015-04:04:03 to 12-25-2015-05:04:03

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
189.199.161.14	147.237.77.74	Mexico	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
112.168.26.199	147.237.77.216	Korea, Republic of	dover.idf.il	ET SCAN Potential SSH Scan	1
112.168.26.199	147.237.76.86	Korea, Republic of	navy.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.181	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.181	147.237.77.121	Netherlands	e.navy.idf.il	ET SCAN Potential SSH Scan	1
42.122.104.170	147.237.76.30	China	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
189.199.161.14	147.237.77.234	Mexico	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.130.5.208	147.237.77.176		matpash.idf.il	ET SCAN NMAP -sS window 1024	1
112.168.26.199	147.237.76.202	Korea, Republic of	e.halag.idf.il	ET SCAN Potential SSH Scan	1
112.168.26.199	147.237.76.44	Korea, Republic of	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.181	147.237.77.178	Netherlands	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
61.244.49.137	147.237.77.176	Hong Kong	matpash.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
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
37.26.147.162	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
80.246.136.100	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
80.246.136.100	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
80.246.136.100	Israel	147.237.72.166	aka.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
40.77.167.21	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
46.19.85.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
37.26.149.144	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		alert	2
80.246.136.100	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
66.249.65.2	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.139	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.26.149.144	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
80.246.136.100	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	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
5.175.193.232	Germany	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
46.19.85.223	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
91.200.12.136	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
199.30.24.226	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
80.246.136.100	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
74.82.47.10	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.168	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.71	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
202.1.197.123	Maldives	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.60	United States	147.237.0.15	kosher-kravi.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
66.240.192.138	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.161	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.26.149.144	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.8.132.22	Russian Federation	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
5.144.60.146	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.236	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.16	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.169	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.96	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
130.193.50.1	Russian Federation	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.162	United States	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.187.114.171	France	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.144.60.146	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
184.105.247.251	United States	147.237.76.147	chimuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.16	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.171	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.99	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
130.193.50.1	Russian Federation	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
216.218.206.100	United States	147.237.77.19	law-forum.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
109.253.220.67	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
146.185.234.48	Russian Federation	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 146.185.234.48	Block	2
2.54.52.177	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/born2.htm	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1153-16883-he/mmmmmmm=d50780f8mmmmmm_d50780f8	Block	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
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
207.46.13.171	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
146.185.234.48	Russian Federation	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/templates/news/news.in.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
77.127.183.7	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
188.143.232.21	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 188.143.232.21	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.66.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
149.78.13.60	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.176.119.190	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sachar	Block	1
188.143.232.21	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/general/general.aspx/templates/sendtofriend/sendtofriend.aspx	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
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.178	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	1
87.69.137.150	Israel	147.237.0.16	my-kosher-kravi.idf.il	Parameter Type Violation returnUrl in my-kosher-kravi.idf.il/templates/login/login.aspx	Block	1
46.117.123.34	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
193.90.12.87	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation pageNum in www.idf.il/1395-en/dover.aspx	Block	1
162.243.188.75	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to /	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
46.166.190.168	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1