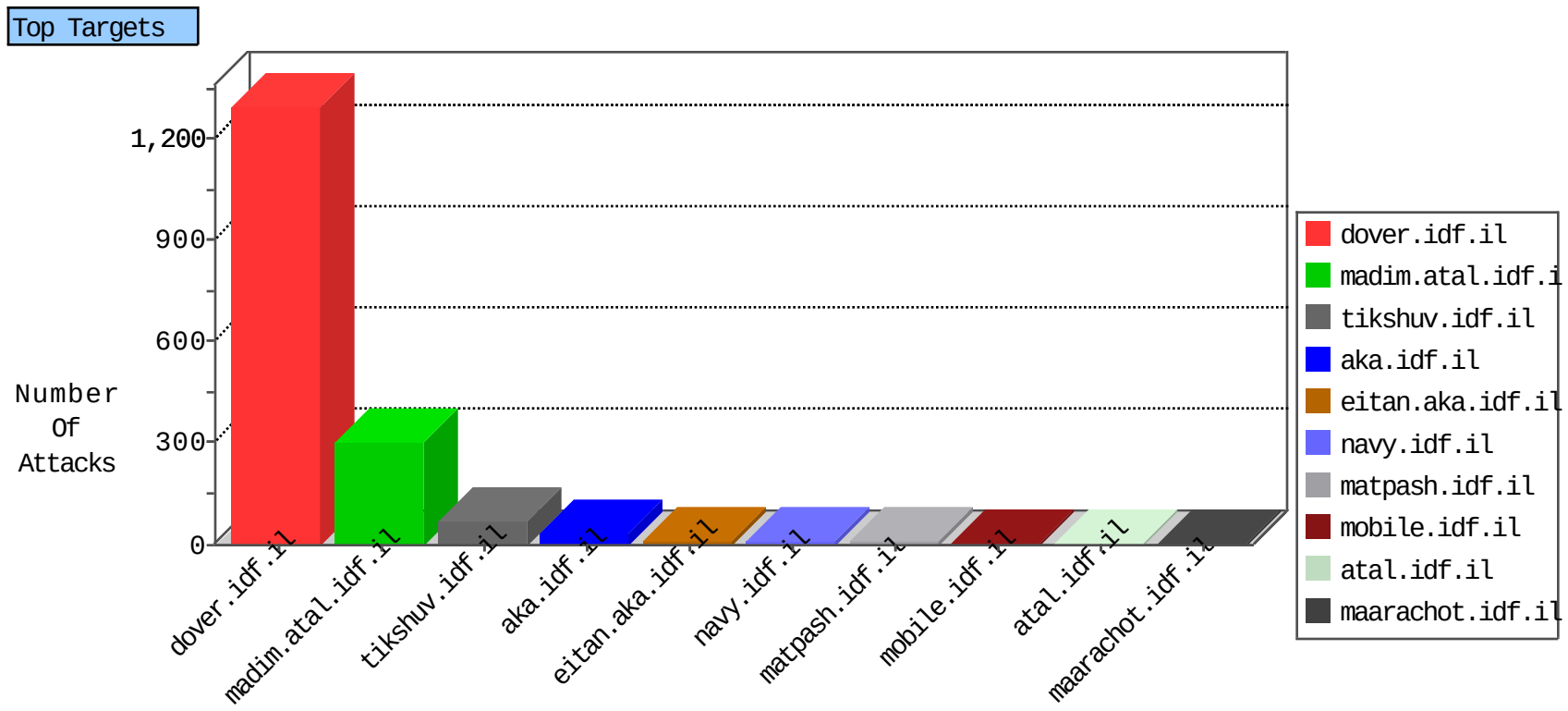
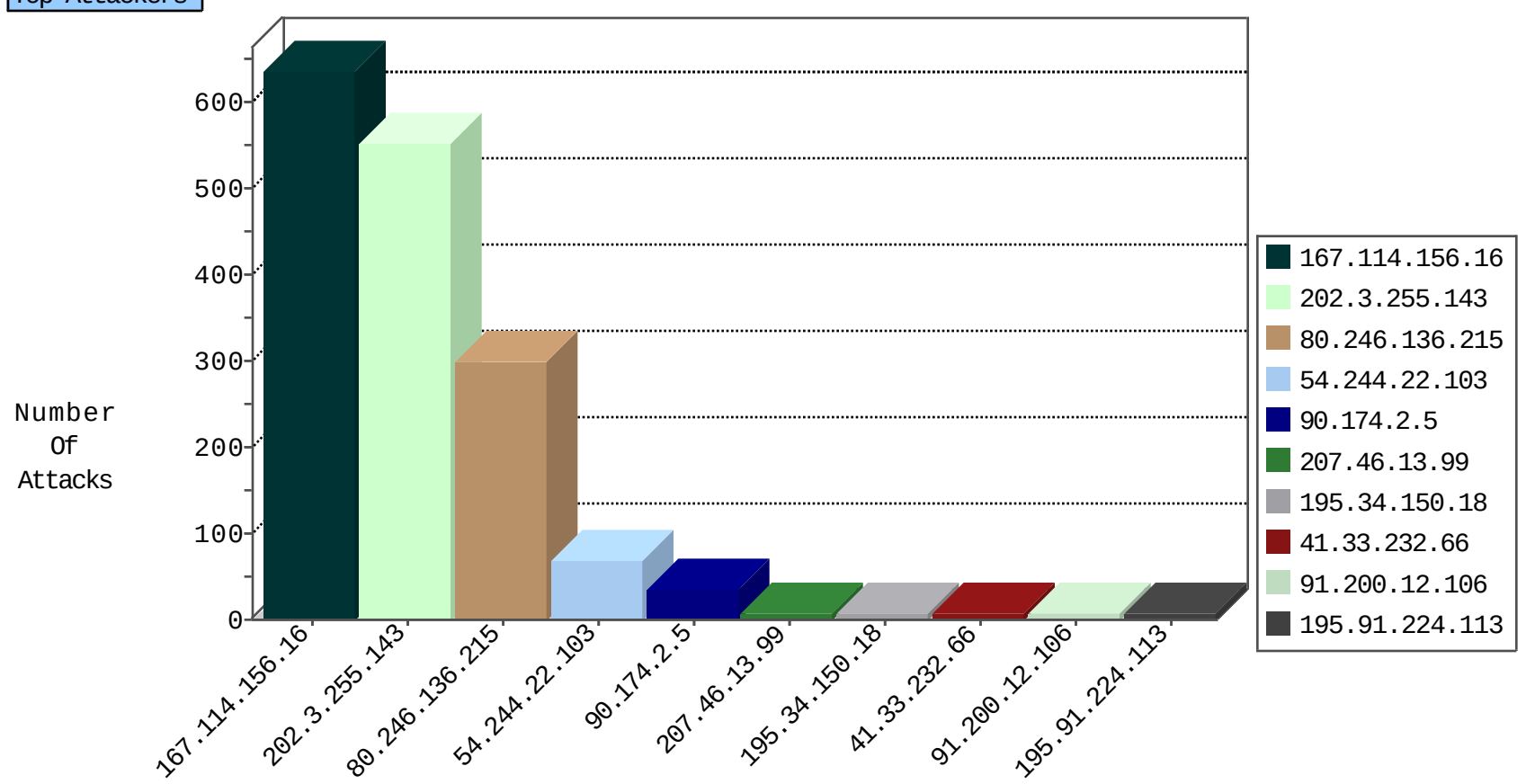
01-16-2016-02:04:00 to 01-16-2016-03:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-16-2016-02:04:00 to 01-16-2016-03:04:00

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	3362
185.62.189.53	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1

01-16-2016-02:04:00 to 01-16-2016-03:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
83.218.232.238	Ukraine	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1

01-16-2016-02:04:00 to 01-16-2016-03:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
202.3.255.143	147.237.77.216	French Polynesia	dover.idf.il	GPL SCAN nmap TCP	512
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
80.246.136.215	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	2
66.249.66.65	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
66.249.66.81	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	2
66.249.64.9	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	2
176.58.106.95	147.237.77.234	United Kingdom	halag.idf.il	ET SCAN Potential SSH Scan	1
104.37.187.183	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 3072	1
89.248.172.98	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
5.39.222.253	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	147.237.77.176	Cote D'Ivoire	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.252.84	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
104.236.63.196	147.237.0.16		my-kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
90.174.2.5	147.237.77.216	Spain	dover.idf.il	portscan: TCP Distributed Portscan	1
82.117.208.243	147.237.77.19		law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
196.47.173.21	147.237.77.176	Cote D'Ivoire	matpash.idf.il	ET SCAN NMAP -sS window 4096	1

01-16-2016-02:04:00 to 01-16-2016-03:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	68
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
90.174.2.5	Spain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
207.46.13.99	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
90.174.2.5	Spain	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
195.91.224.113	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
90.174.2.5	Spain	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
90.174.2.5	Spain	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
96.36.139.162	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.180.151.243	Israel	147.237.72.166	aka.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.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.62.248	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
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
37.26.148.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
198.48.233.116	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
157.55.39.230	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
122.178.68.12	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
157.55.39.13	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
206.253.224.14	United States	147.237.72.14	dover.idf.il(old	Bad TCP sequence	SYN retransmit with different window scale	monitor	2
169.0.177.135		147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
37.26.148.217	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
90.174.2.5	Spain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
198.48.233.116	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.177.35.98	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.86.36	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
2.52.63.117	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
217.132.100.243	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.178	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
79.177.35.98	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
5.102.253.87	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
90.174.2.5	Spain	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	1
220.181.108.96	China	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.85.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
8.37.227.69	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	1
195.154.227.118	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
46.19.85.119	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
157.55.39.53	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.215	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 80.246.136.215	Block	186
80.246.136.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
80.246.136.215	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 80.246.136.215	Block	7
2.52.62.248	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
208.80.155.132	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	2
173.252.115.84	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
173.252.115.90	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/edim/yoman/yoman.asp	Block	1
195.154.194.111	France	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	1
150.70.97.84	Japan	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
40.77.167.43	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
68.142.232.26	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 68.142.232.26	Block	1
195.154.194.111	France	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/wp-login.php	Block	1
150.70.97.84	Japan	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/1133-22461-he/dover.aspx.	Block	1
208.113.198.103	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/wp/wp-admin/	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
173.252.115.85	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
104.236.63.196		147.237.0.16	my-kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
68.142.232.26	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/wp-admin/	Block	1
195.154.226.90	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
155.94.65.186	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/test/wp-admin/	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
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/haredim/haredim.aspx	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
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1133-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
5.152.192.218	United Kingdom	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/wordpress/wp-admin/	Block	1
157.55.39.101	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
184.172.172.26	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/old/wp-admin/	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
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1100-he/nakhal.aspx	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
31.131.72.45	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi'a=0	Block	1
157.55.39.175	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.maarachot.idf.il/pdf/files/5/112435.pdf).	Block	1