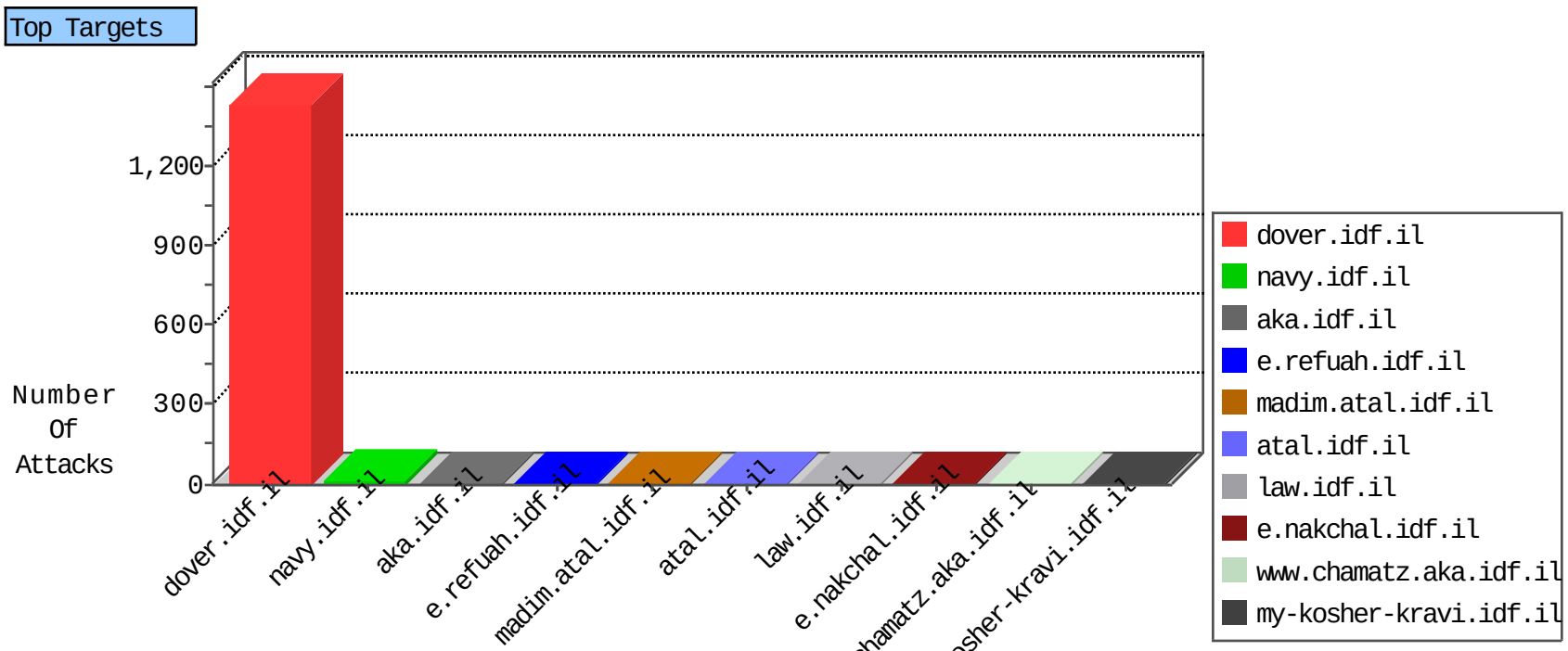
01-16-2016-05:04:01 to 01-16-2016-06:04:01

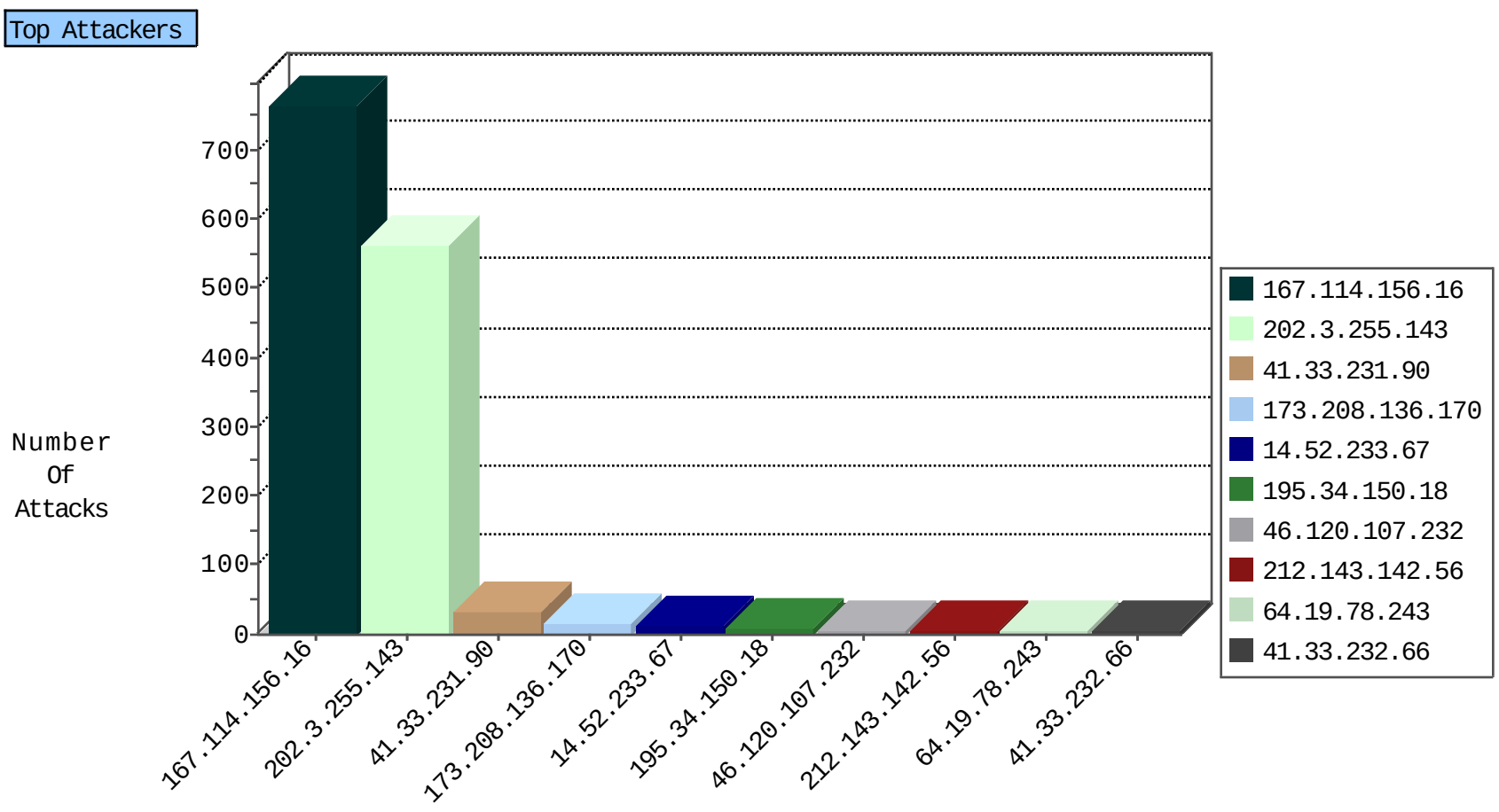
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-16-2016-05:04:01 to 01-16-2016-06:04:01

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	3061

01-16-2016-05:04:01 to 01-16-2016-06:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
14.52.233.67	Korea, Republic of	147.237.77.216	dover.idf.il	9310: HTTP: Suspicious HTTP Request	Permit	1

01-16-2016-05:04:01 to 01-16-2016-06:04:01

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	524
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
41.140.253.9	147.237.76.199	Morocco	e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
218.246.0.97	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
176.58.106.95	147.237.76.202	United Kingdom	e.halag.idf.il	ET SCAN Potential SSH Scan	1
168.62.238.153	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
114.112.90.54	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.76.34	Ukraine	yohalan.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
82.117.208.243	147.237.8.46		e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
41.140.253.9	147.237.76.199	Morocco	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
41.140.253.9	147.237.76.199	Morocco	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
218.246.0.97	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
176.58.106.95	147.237.0.19	United Kingdom	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
168.62.238.153	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
82.166.184.187	147.237.0.200	Israel	m4u.idf.il	ET SCAN NMAP -sS window 4096	1
45.79.183.130	147.237.77.170		maarachot.idf.il	ET SCAN Potential SSH Scan	1

01-16-2016-05:04:01 to 01-16-2016-06:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
64.19.78.243	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
173.208.136.170	United States	147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
173.208.136.170	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
157.55.39.174	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
169.0.177.135		147.237.77.216	dover.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
46.120.107.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.109.68.35	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
75.126.221.55	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
46.120.107.232	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
75.126.221.55	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
74.82.47.6	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
216.218.206.90	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.82	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
52.53.218.29	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
208.115.113.89	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.14	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.102	United States	147.237.0.35	akaws.idf.il	drop		drop	1
184.105.247.220	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.75.199.187	China	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.113.89	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
74.82.47.22	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.108	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.252	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.179	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
65.19.167.132	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
216.218.206.111	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.180	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
68.190.208.233	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
14.52.233.67	Korea, Republic of	147.237.77.216	dover.idf.il	PHP Attempt	Block	5
14.52.233.67	Korea, Republic of	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 14.52.233.67	Block	4
157.55.39.230	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19149-he/dover	Block	1
104.236.227.151		147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/894-he/nakhal.aspxshared/usercontrols/headerupper/	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
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
173.208.136.170	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/ftb.imagegallery.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
104.236.31.180		147.237.0.16	my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unsupported Cipher	None	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/8/kkkkkkk=074de65fkkkkkkk_074de65f	Block	1
159.203.105.189	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Unsupported Cipher	None	1
106.75.199.187	China	147.237.0.19	madim.atal.idf.il	Distributed Unauthorized URL Access on 147.237.0.19/	Block	1
67.19.79.218	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	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
173.208.136.170	United States	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
141.212.122.177	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
104.236.71.39		147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Unsupported Cipher	None	1
188.143.232.40	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 188.143.232.40	Block	1
159.203.110.232	United States	147.237.76.39	mobile.meitav.idf.il	Untraceable SSL Sessions: Unsupported Cipher	None	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
74.82.47.2	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	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
173.208.136.170	United States	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 173.208.136.170	Block	1
157.55.39.98	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam/main/procedure.asp	Block	1
104.236.73.21		147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Unsupported Cipher	None	1
188.143.232.40	Russian Federation	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/searchresults/searchresults.aspx/templates/sendtofriend/sendtofriend.aspx	Block	1
14.52.233.67	Korea, Republic of	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-content/uploads/info.php	Block	1
173.208.136.170	United States	147.237.76.86	navy.idf.il	Multiple Admin Blocking from 173.208.136.170	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
81.7.15.115	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
173.208.136.170	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 173.208.136.170	Block	1
157.55.39.230	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.230	Block	1
104.236.82.76		147.237.0.16	my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unsupported Cipher	None	1
195.154.83.161	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1086-he/dover.aspx	Block	1
173.208.136.170	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 173.208.136.170	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
95.130.13.157	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
178.20.55.18	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1