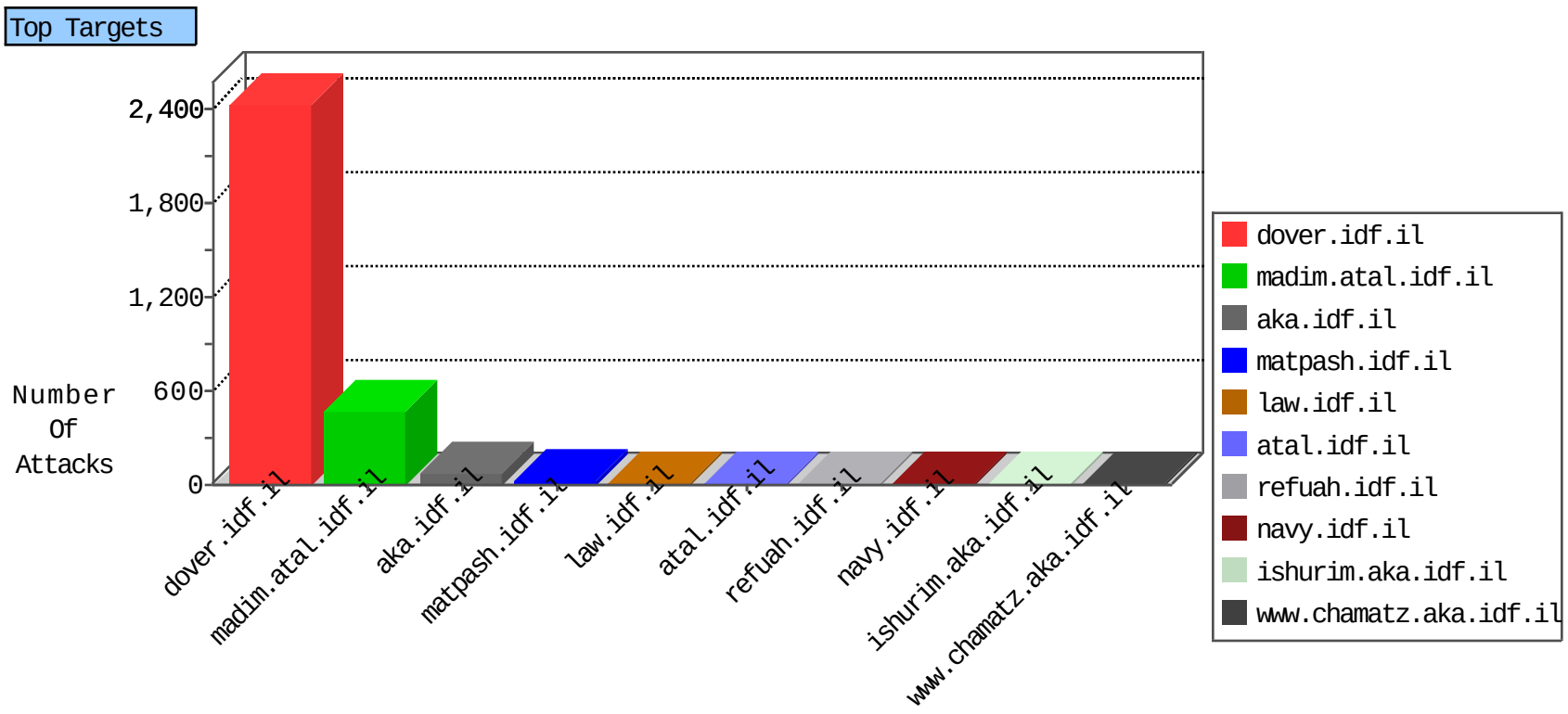
01-21-2016-12:04:06 to 01-21-2016-13:04:06

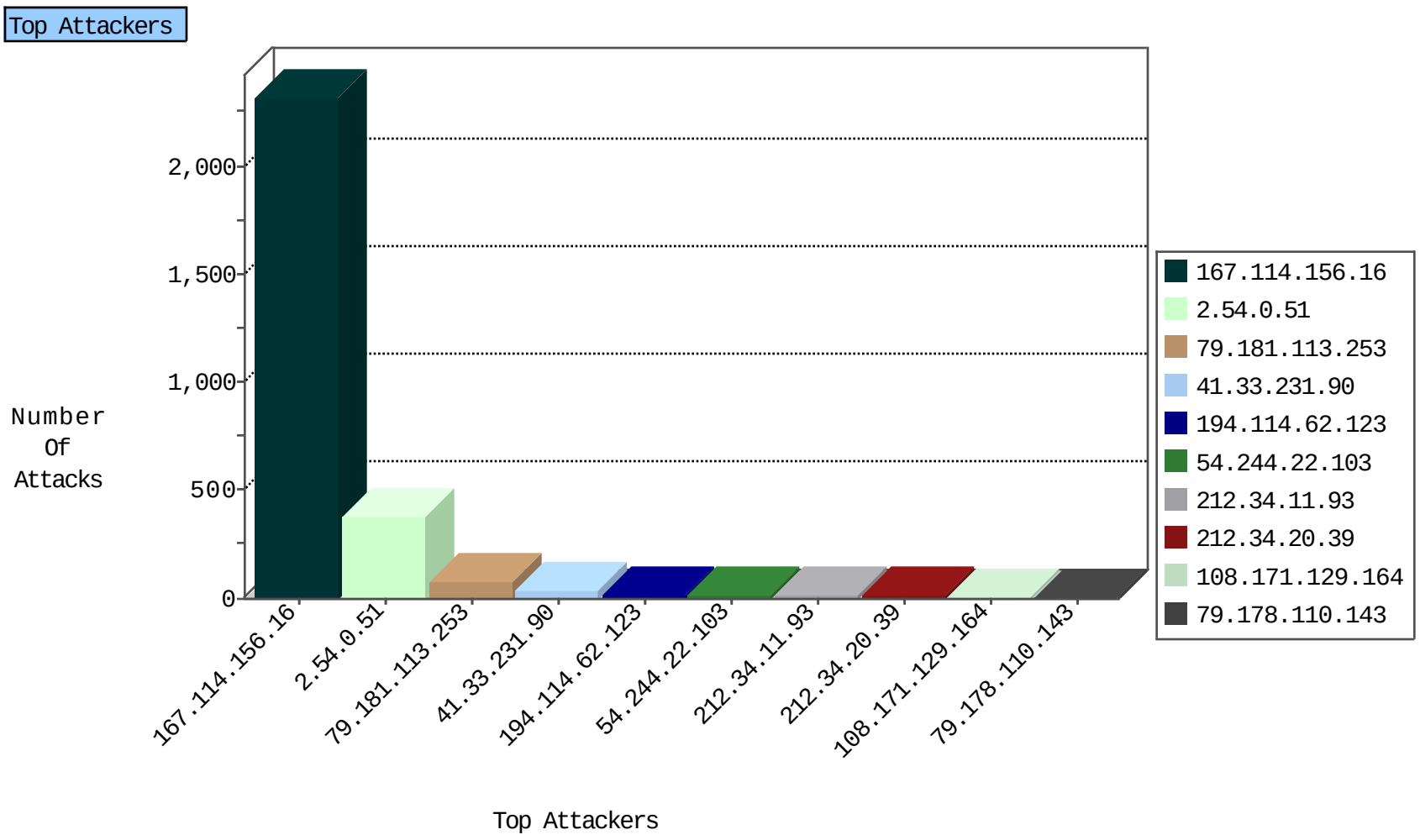
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-21-2016-12:04:06 to 01-21-2016-13:04:06

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	3095
66.249.78.2	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	2881
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
142.54.169.165	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	drop	1
115.230.124.164	China	147.237.76.201	e.atal.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
119.77.224.237	Taiwan	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
141.212.122.157	United States	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
74.91.28.61	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	drop	1

01-21-2016-12:04:06 to 01-21-2016-13:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.50.134.71	Canada	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1

01-21-2016-12:04:06 to 01-21-2016-13:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
217.132.154.20	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.191.56.187	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1
199.191.56.187	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -f -sS	1
146.185.250.2	147.237.77.121	Russian Federation	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.79.79	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sA (2)	1
218.246.0.97	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
212.179.102.167	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.191.56.187	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
105.156.43.242	147.237.76.42	Morocco	refuah.idf.il	Tehila - Perl LWP with fake user agent	1
79.177.27.198	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.91.31	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

01-21-2016-12:04:06 to 01-21-2016-13:04:06

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
194.114.62.123	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	8
62.0.200.200	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.242	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
217.194.203.52	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
82.166.93.161	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
185.120.125.25		147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
95.27.60.165	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
193.105.134.220	Sweden	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
141.212.121.192	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
62.219.184.130	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
31.154.5.242	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
213.8.41.69	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
193.105.134.220	Sweden	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
81.169.237.146	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	1
37.142.196.18	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
216.243.31.2	United States	147.237.0.33	idf.il	drop		drop	1
193.105.134.220	Sweden	147.237.76.34	yohalan.idf.il	drop	SAM rule	drop	1
82.239.61.19	France	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
193.105.134.220	Sweden	147.237.77.235	sviva.idf.il	drop	SAM rule	drop	1
157.55.39.73	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	1
81.169.237.146	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
216.243.31.2	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
193.105.134.220	Sweden	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	1
169.229.3.91	United States	147.237.0.200	m4u.idf.il	drop		drop	1
81.169.237.146	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	1
46.19.85.7	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
193.105.134.220	Sweden	147.237.76.39	mobile.meitav.idf.il	drop	SAM rule	drop	1
115.230.124.164	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
62.219.13.180	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
185.120.125.25		147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
82.81.66.116	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

01-21-2016-12:04:06 to 01-21-2016-13:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.0.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	187
2.54.0.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
2.54.0.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	78
79.181.113.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	70
84.108.213.22	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
108.171.129.164	Germany	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 108.171.129.164	Block	5
212.34.11.93	Jordan	147.237.77.216	dover.idf.il	Multiple Malformed URL from 212.34.11.93	Block	4
212.34.11.93	Jordan	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 212.34.11.93	Block	4
109.186.164.109	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/9/2479.jpg	Block	4
46.19.85.200	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	3
212.34.20.39	Jordan	147.237.77.176	matpash.idf.il	Distributed Illegal HTTP Version	Block	3
46.19.85.4	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.9.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.34.20.39	Jordan	147.237.77.176	matpash.idf.il	Distributed Malformed URL	Block	3
212.34.20.39	Jordan	147.237.77.176	matpash.idf.il	Distributed Unknown HTTP Request Method	Block	3
108.171.129.164	Germany	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/	Block	3
46.120.212.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.154.131	Israel	147.237.76.39	mobile.meitav.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtPassword in mobile.meitav.idf.il/templates/login.aspx	Block	2
2.52.37.207	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
41.232.120.5	Egypt	147.237.77.74	law.idf.il	PHP Attempt	Block	2
84.229.30.17	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.253.136.253	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.34.20.39	Jordan	147.237.77.176	matpash.idf.il	Abnormally Long Request method	Block	1
117.103.185.20	Japan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
2.52.0.197	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.178.110.143	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
192.117.176.82	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
37.142.165.181	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.67.42.7	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.28.139.168	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
105.156.43.242	Morocco	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
77.237.138.202	Czech Republic	147.237.77.233	atal.idf.il	Unauthorized URL Access to /	Block	1
184.105.247.195	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
91.121.83.118	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 91.121.83.118	Block	1
212.76.104.195	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-15769-he/dover.aspx&sa=u&ved=0ahukewjdi7aq3rrkahwcshqkhrg4clkqfggsmau&usg=afqjcnfgbcvbdfqjn30_bxz4gzcuk1kdnw	Block	1
54.173.223.170	United States	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.77.74	law.idf.il	Abnormally Long Request method	Block	1
46.19.85.2	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtContent in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
109.253.138.5	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 109.253.138.5	Block	1
212.34.11.93	Jordan	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 212.34.11.93	Block	1
192.117.176.82	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
37.9.122.202	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
79.178.110.143	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docid in www.aka.idf.il/main/giyus/general.aspx	None	1
176.13.7.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.130.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
94.23.27.166	France	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/templates/shared/usercontrols/headerupper/	Block	1
2.52.36.26	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

01-21-2016-12:04:06 to 01-21-2016-13:04:06