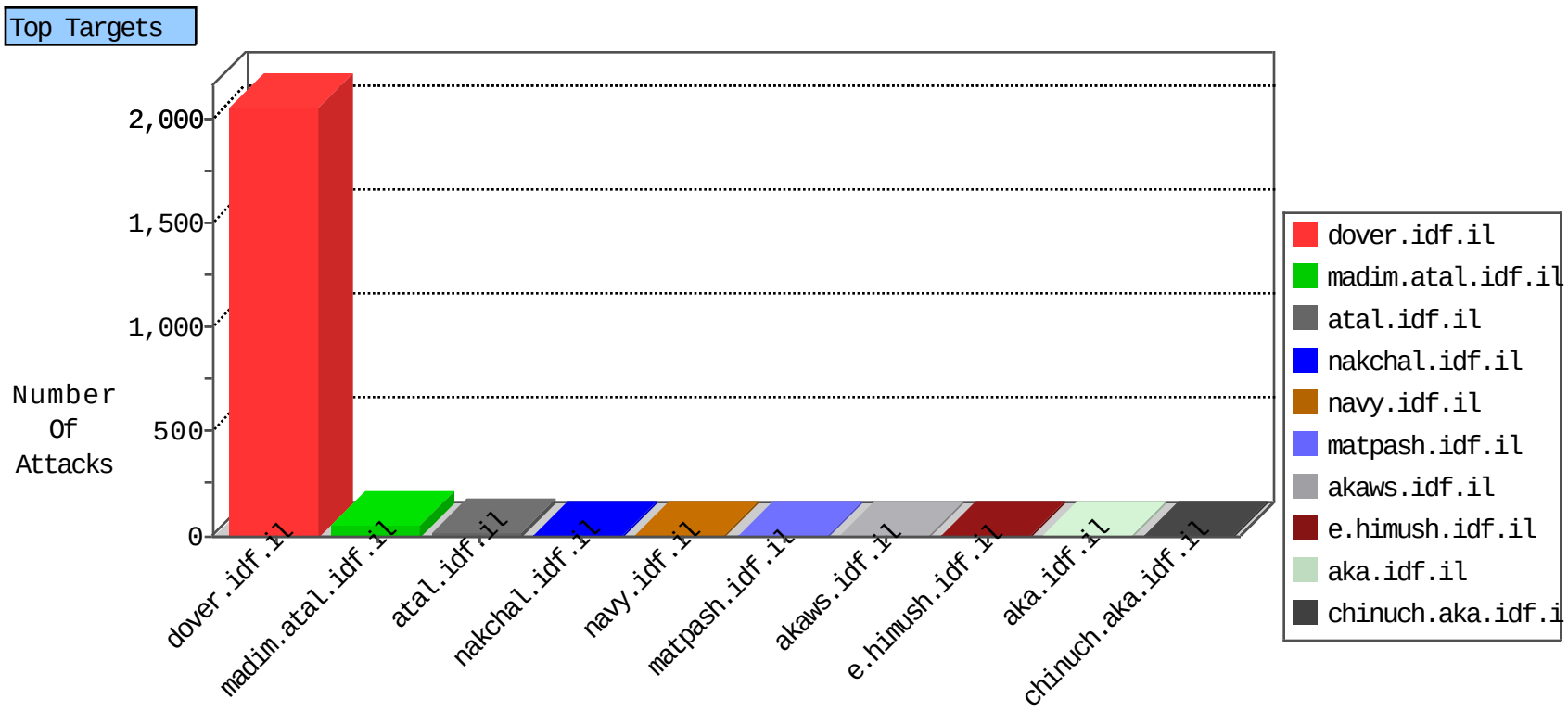
01-07-2016-04:04:08 to 01-07-2016-05:04:08

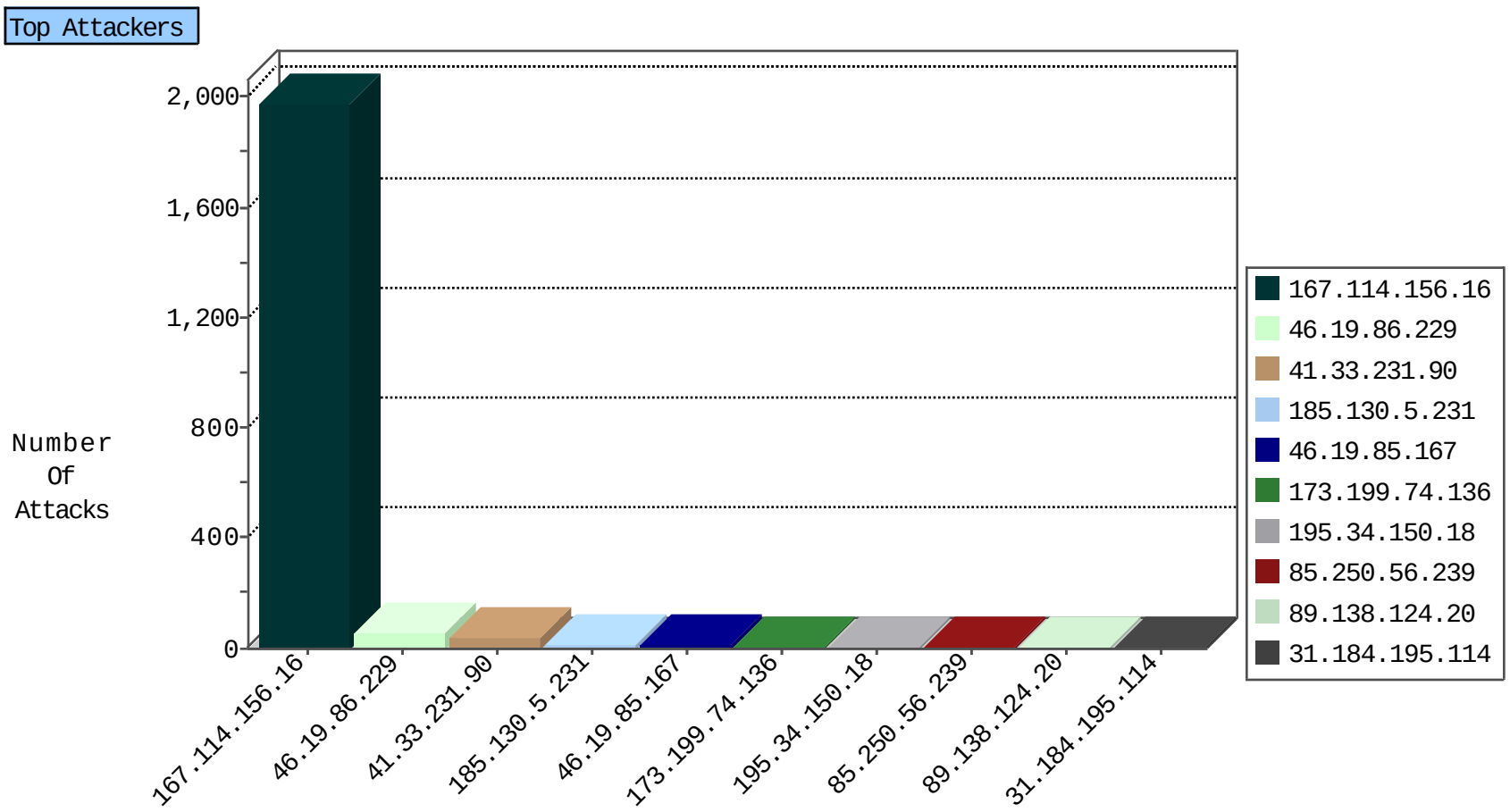
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

01-07-2016-04:04:08 to 01-07-2016-05:04:08

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	3488
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
183.60.48.25	China	147.237.76.196	e.sviva.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
208.67.1.60	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
208.67.1.60	United States	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
89.248.174.4	Netherlands	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
208.67.1.60	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
89.248.174.4	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
208.67.1.60	United States	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	1

01-07-2016-04:04:08 to 01-07-2016-05:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.252.131.34	Germany	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
203.78.12.21	Singapore	147.237.77.170	maarachot.idf.il	12347: HTTP: PHP-CGI Query String Parameter Information Disclosure Vulnerability	Block	1

01-07-2016-04:04:08 to 01-07-2016-05:04:08

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
66.249.93.37	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sA (2)	2
173.199.74.136	147.237.72.14	United Kingdom	dover.idf.il(old)	ET SCAN Potential VNC Scan 5900-5920	1
173.199.74.136	147.237.8.46	United Kingdom	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
172.245.11.57	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 3072	1
104.128.144.131	147.237.76.176	Canada	test.ncore.idf.il	ET SCAN NMAP -sS window 3072	1
209.126.116.147	147.237.77.19	United States	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.195.114	147.237.77.212	Russian Federation	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
31.184.195.114	147.237.76.44	Russian Federation	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
190.65.38.130	147.237.0.33	Colombia	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
31.184.195.114	147.237.0.35	Russian Federation	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.199.74.136	147.237.76.200	United Kingdom	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.199.74.136	147.237.76.39	United Kingdom	mobile.meitav.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
173.199.74.136	147.237.8.50	United Kingdom	e.tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.199.74.136	147.237.0.35	United Kingdom	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
172.245.11.57	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
201.160.77.135	147.237.0.15	Mexico	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
31.184.195.114	147.237.76.201	Russian Federation	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
193.105.134.220	147.237.77.243	Sweden	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.195.114	147.237.8.46	Russian Federation	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.199.74.136	147.237.77.178	United Kingdom	e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
31.184.195.114	147.237.0.34	Russian Federation	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
173.199.74.136	147.237.76.197	United Kingdom	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

01-07-2016-04:04:08 to 01-07-2016-05:04:08

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
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
85.250.56.239	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
46.19.85.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
89.138.124.20	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
207.46.13.32	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	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
207.46.228.208	United States	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
207.46.228.208	United States	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	2
188.143.232.16	Russian Federation	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
77.237.138.202	Czech Republic	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
184.105.139.84	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
93.174.93.203	Netherlands	147.237.76.30	himush.idf.il	drop	SAM rule	drop	1
185.130.5.231		147.237.76.148	gqcenter.aka.idf.il	drop	SAM rule	drop	1
185.130.5.231		147.237.0.35	akaws.idf.il	drop	SAM rule	drop	1
141.212.122.175	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
198.20.69.74	United States	147.237.8.28	e.mobile-ks.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
81.44.224.176	Spain	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
185.130.5.231		147.237.76.202	e.halag.idf.il	drop	SAM rule	drop	1
185.130.5.231		147.237.76.42	refuah.idf.il	drop	SAM rule	drop	1
184.105.139.112	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
115.230.126.48	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
193.105.134.220	Sweden	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.61	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.130.5.231		147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	1
185.130.5.231		147.237.76.30	himush.idf.il	drop	SAM rule	drop	1
149.50.101.223	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
199.30.24.141	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
85.65.6.28	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.130.5.231		147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
45.79.168.168		147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
185.130.5.231		147.237.76.44	e.refuah.idf.il	drop	SAM rule	drop	1
184.105.247.220	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
212.83.40.238	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.160	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
193.105.134.220	Sweden	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.52	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.130.5.231		147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
185.130.5.231		147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
199.30.24.141	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
188.143.232.16	Russian Federation	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
46.19.85.63	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
185.130.5.231		147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
184.105.247.220	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.165	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
193.105.134.220	Sweden	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.130.5.231		147.237.76.197	e.himush.idf.il	drop	SAM rule	drop	1

01-07-2016-04:04:08 to 01-07-2016-05:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
109.253.145.80	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
207.46.13.123	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.123	Block	1
89.138.124.20	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
116.25.105.70	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-ar/cogat.aspx	Block	1
207.46.13.157	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
91.196.50.33	Poland	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to testp3.pospr.waw.pl/testproxy.php	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
151.80.138.19	Italy	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
74.82.47.4	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
207.46.13.157	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20168-he/girls02.php	Block	1
91.196.50.33	Poland	147.237.76.30	himush.idf.il	Unauthorized URL Access to testp2.czar.bielawa.pl/testproxy.php	Block	1
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
176.10.104.240	Switzerland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.181.161.254	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
207.46.228.208	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
188.76.241.119	Spain	147.237.77.176	matpash.idf.il	Web leech 7	Block	1
85.250.56.239	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
207.241.237.211	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/3sandsafety/q3-f.ilh.jowh	Block	1
115.230.126.48	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ckfinder	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1934-he/cogat.aspx	Block	1

01-07-2016-04:04:08 to 01-07-2016-05:04:08