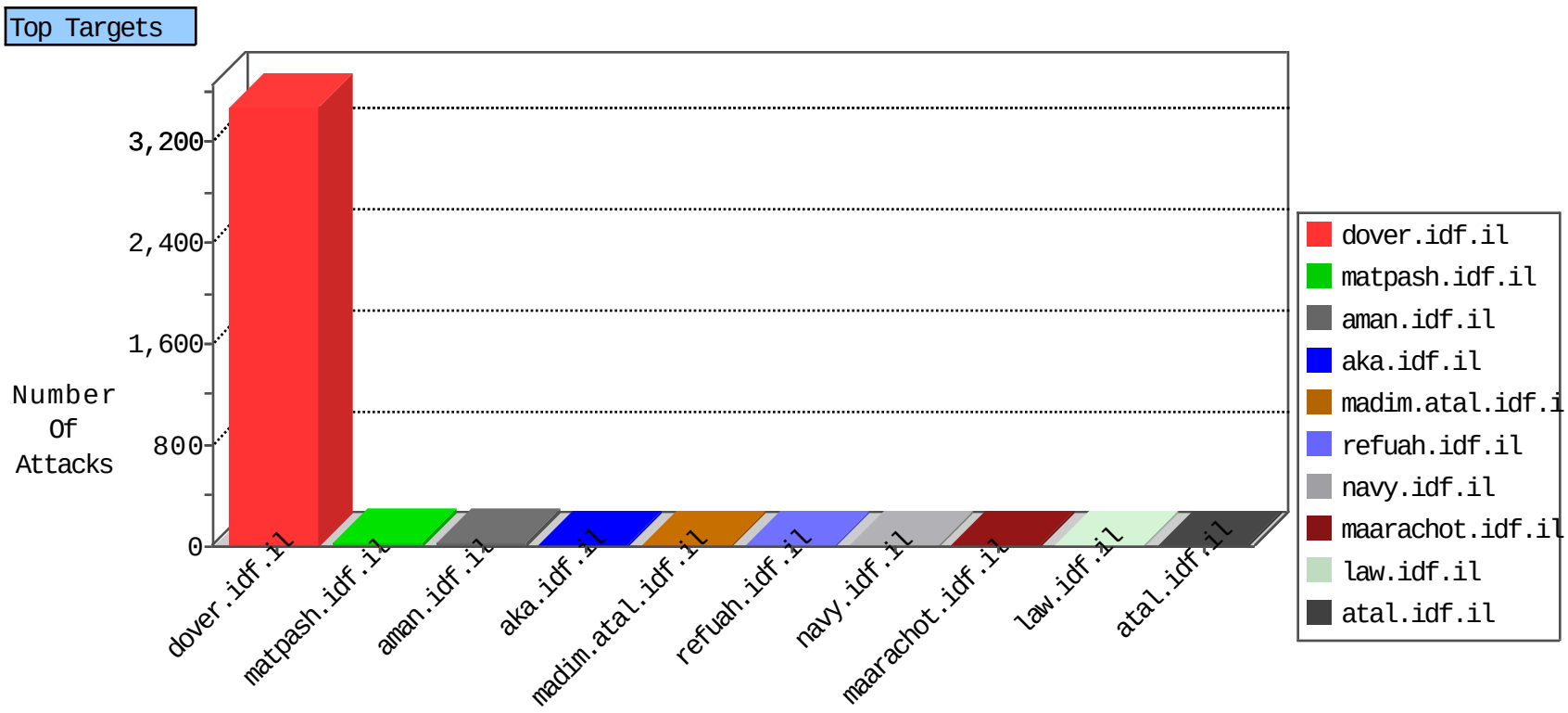
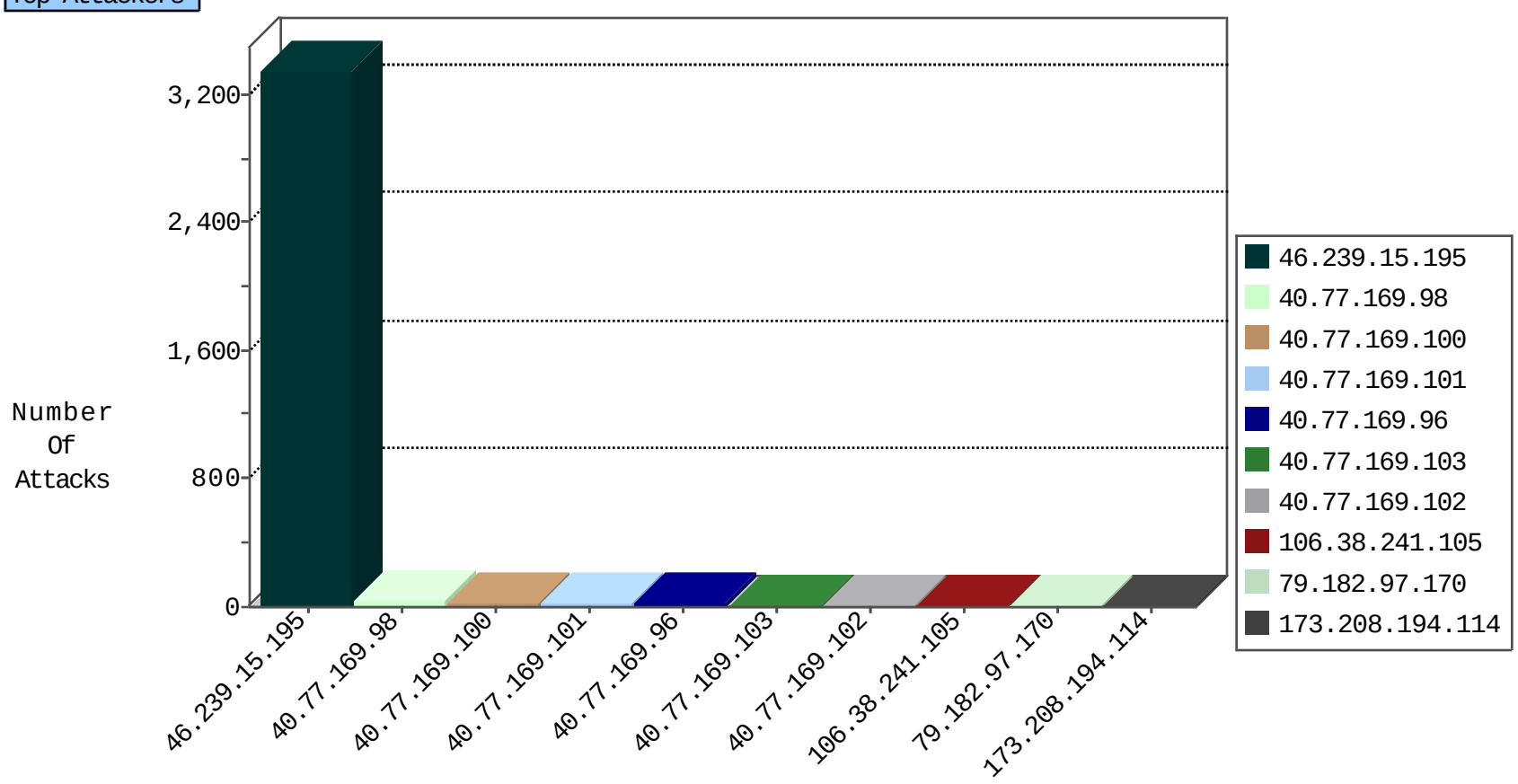
08-28-2016-01:05:12 to 08-28-2016-02:05:12

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-28-2016-01:05:12 to 08-28-2016-02:05:12

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	Frk_Under_Attack_Con_Http	drop	2
185.94.111.1	Russian Federation	147.237.76.177	ncore.idf.il	Black List	drop	1

08-28-2016-01:05:12 to 08-28-2016-02:05:12

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
173.208.194.114	United States	147.237.72.156	aman.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
78.181.63.184	Turkey	147.237.72.166	aka.idf.il	C1000016: HTTP: administrator in URI	Permit	1
78.181.63.184	Turkey	147.237.72.166	aka.idf.il	C1000018: HTTP: access to administrator/index.php -> Quarantine	Permit	1
173.208.194.114	United States	147.237.72.156	aman.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1

08-28-2016-01:05:12 to 08-28-2016-02:05:12

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.64.112	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sA (2)	2
123.249.0.33	147.237.72.156	China	aman.idf.il	ET SCAN Potential SSH Scan	1
106.3.132.14	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
183.129.160.229	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
173.208.194.114	147.237.72.156	United States	aman.idf.il	ET WEB_SERVER Muieblackcat scanner	1
50.84.213.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 3072	1
163.172.169.150	147.237.8.27	United Kingdom	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.0.35	United Kingdom	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
154.16.199.174	147.237.77.235	United States	sviva.idf.il	ET SCAN Potential SSH Scan	1
125.77.28.26	147.237.72.166	China	aka.idf.il	ET SCAN Potential SSH Scan	1
123.249.0.33	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
123.249.0.33	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
186.170.182.146	147.237.77.216	Colombia	dover.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.81.215	147.237.77.216	Russian Federation	dover.idf.il	ET SCAN NMAP -sA (2)	1
183.129.160.229	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
50.84.213.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 4096	1
163.172.220.43	147.237.77.233	United Kingdom	atal.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.0.35	United Kingdom	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.169.150	147.237.0.19	United Kingdom	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
125.77.28.26	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
123.249.0.33	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1

08-28-2016-01:05:12 to 08-28-2016-02:05:12

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3203
46.239.15.195	Bosnia and Herzegovina	147.237.77.216	dover.idf.il	drop		drop	150
40.77.169.98	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
40.77.169.100	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	15
40.77.169.103	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	13
40.77.169.100	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	11
40.77.169.102	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	10
79.182.97.170	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	10
40.77.169.96	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	9
40.77.169.101	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	9
40.77.169.96	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	7
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
40.77.169.98	United States	147.237.72.156	aman.idf.il	drop	SAM rule	drop	6
40.77.169.97	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.65	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	3
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop		drop	2
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
106.38.241.105	China	147.237.72.156	aman.idf.il	drop	SAM rule	drop	2
106.38.241.105	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
40.77.169.102	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	2
106.38.241.105	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
106.38.241.105	China	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
109.226.40.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
106.38.241.105	China	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
106.38.241.105	China	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
40.77.169.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
128.232.110.28	United Kingdom	147.237.0.200	m4u.idf.il	drop		drop	1
106.38.241.105	China	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
66.249.69.109	Israel	147.237.0.33	idf.il	drop		drop	1
128.232.110.28	United Kingdom	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
106.38.241.105	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
212.76.104.102	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
106.38.241.105	China	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1

08-28-2016-01:05:12 to 08-28-2016-02:05:12

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
40.77.169.99	United States	147.237.77.216	dover.idf.il	Distributed Illegal Byte Code Character in URL	Block	6
31.210.187.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.178.39.142	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation searchText in www.refua.atal.idf.il/1221-he/refuah.aspx	Block	2
2.53.45.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	2
131.253.27.93	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
77.139.143.26	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	2
88.167.160.151	France	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/topic.php	Block	1
58.98.155.39	Japan	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/wp-login.php	Block	1
66.249.76.74	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/.well-known/apple-app-site-association	Block	1
46.19.86.93	Israel	147.237.76.147	chinuch.aka.idf.il	Malformed URL	Block	1
88.167.160.151	France	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/wp-login.php	Block	1
72.199.149.86	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
66.220.156.101	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/sip_storage/files/9/size220x0/2019.jpg	Block	1
80.246.133.159	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/homepage/homepage.aspx	Block	1
46.19.86.93	Israel	147.237.76.147	chinuch.aka.idf.il	Unknown HTTP Request Method deflate in URL	Block	1
73.110.34.216	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
66.249.64.58	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/.well-known/assetlinks.json	Block	1
5.102.195.78	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
85.222.58.162	Poland	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.106	Block	1
46.97.121.94	Romania	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.173	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
77.139.143.26	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.139.143.26	Block	1
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
85.222.58.162	Poland	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.maarachot.idf.il/wp-login.php	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
58.98.155.39	Japan	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
207.46.13.109	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
66.249.76.46	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/giyus/asp/rec.asp	Block	1

08-28-2016-01:05:12 to 08-28-2016-02:05:12