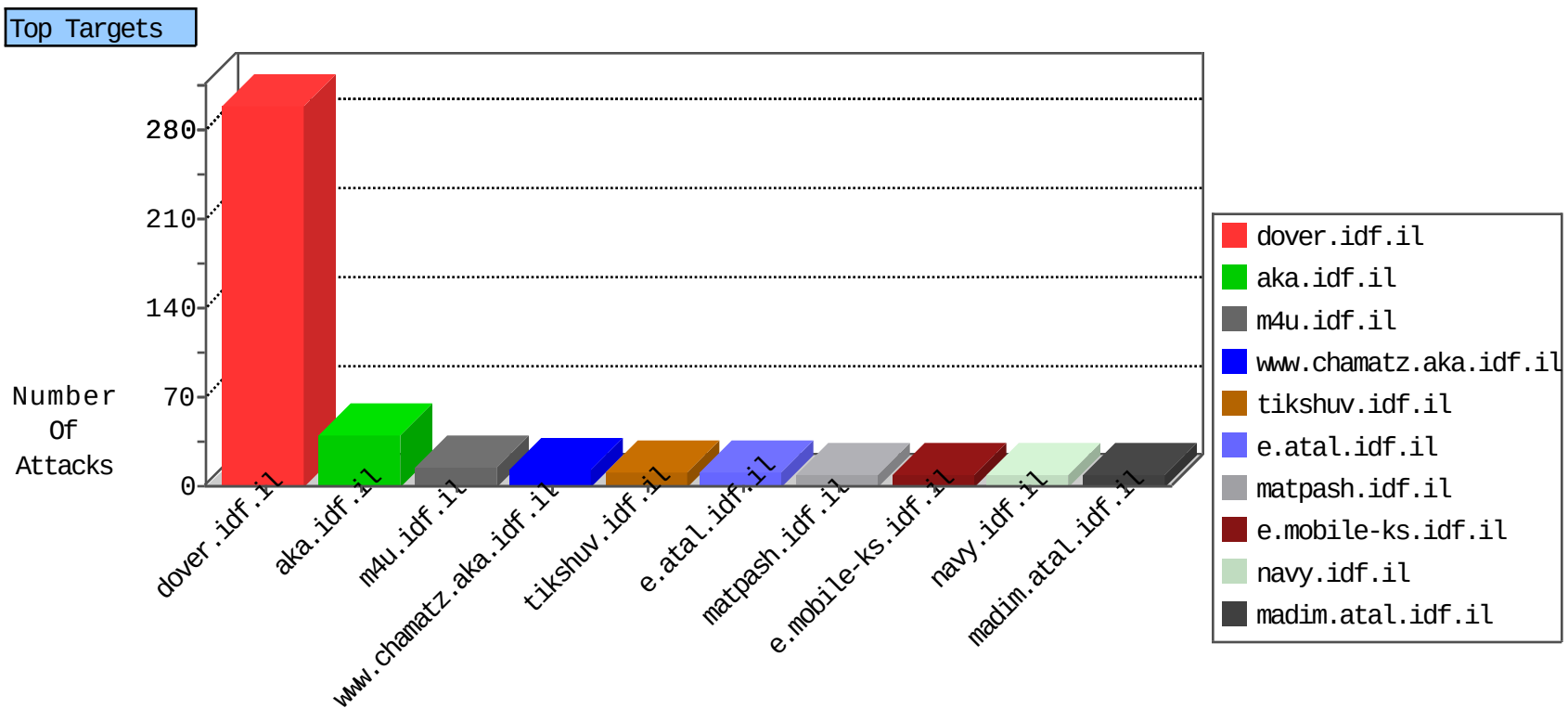
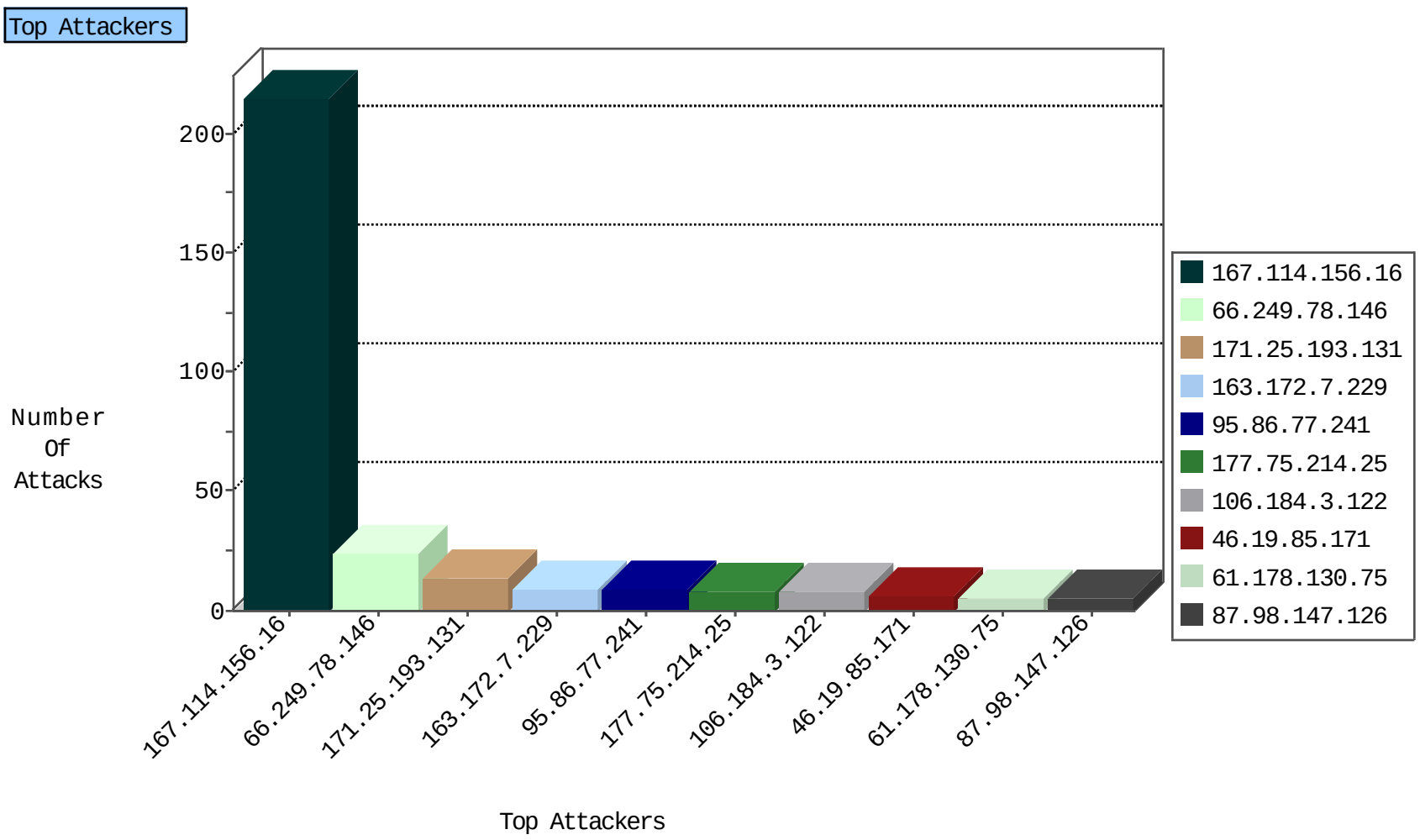
04-20-2016-04:04:04 to 04-20-2016-05:04:04

IDF Under Attack Daily Report





04-20-2016-04:04:04 to 04-20-2016-05:04:04

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	1011
167.114.156.16	Canada	147.237.77.216	dover.idf.il	JLM_Under_Attack_Con_Http	drop	4

04-20-2016-04:04:04 to 04-20-2016-05:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
203.206.226.146	Australia	147.237.0.34	tikshuv.idf.il	3885: HTTP: PHP File Include Exploit	Block	2
203.206.226.146	Australia	147.237.0.34	tikshuv.idf.il	4807: HTTP: PHP File Include Exploit	Block	1

04-20-2016-04:04:04 to 04-20-2016-05:04:04

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
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	4
117.34.70.143	147.237.8.45	China	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
107.158.255.194	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
80.82.78.38	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
13.92.245.177	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 4096	1
117.34.70.143	147.237.8.27	China	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
107.158.255.194	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -f -sS	1
13.92.245.177	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 3072	1

04-20-2016-04:04:04 to 04-20-2016-05:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	117
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
95.86.77.241	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
171.25.193.131	Sweden	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
163.172.7.229	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.171	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
61.178.130.75	China	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
10.0.0.6		147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	4
183.104.100.66	Korea, Republic of	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
66.249.79.102	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.66.11.145	Denmark	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
95.242.241.172	Italy	147.237.77.170	maarachot.idf.il	drop		drop	3
106.184.3.122	Japan	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
201.205.142.206	Costa Rica	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
178.21.55.21	Hungary	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
37.9.122.202	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.97.198.228	Turkey	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
114.32.219.204	Taiwan	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
13.92.245.177	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
118.68.215.174	Vietnam	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
91.200.12.136	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
187.22.50.161	Brazil	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
189.61.131.147	Brazil	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
14.169.67.54	Vietnam	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
187.66.194.144	Brazil	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
207.46.13.95	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
109.251.210.23	Ukraine	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
220.132.207.234	Taiwan	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
37.26.149.206	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
213.14.190.73	Turkey	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
211.21.223.234	Taiwan	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
36.233.79.105	Taiwan	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
187.181.235.64	Brazil	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
186.233.181.160	Brazil	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
1.55.141.115	Vietnam	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
66.87.116.113	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
106.186.113.132	Japan	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.27	United States	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
212.76.127.219	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
84.232.253.81	Romania	147.237.77.179	e.mazi.idf.il	drop		drop	1
104.148.44.148	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
122.54.117.24	Philippines	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
177.75.214.25	Brazil	147.237.0.33	idf.il	drop		drop	1
205.168.84.133	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
37.105.145.110	Saudi Arabia	147.237.77.176	matpash.idf.il	drop		drop	1
74.82.47.50	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
93.115.95.207	Anonymous Proxy	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
171.25.193.131	Sweden	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
188.120.148.139	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

04-20-2016-04:04:04 to 04-20-2016-05:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.109.207.221	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 208.109.207.221	Block	3
219.94.162.100	Japan	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp-admin/	Block	1
157.55.39.223	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/templatecontrols/newsflash/www.ynet.co.il	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
40.77.167.104	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/main/haredim/general.aspx	None	1
207.46.13.184	United States	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/templates/general/general.aspx	Block	1
106.184.3.122	Japan	147.237.77.226	www.chamatz.aka.idf.il	Abnormally Long Request method	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
163.172.7.229	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
97.74.24.225	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
46.19.86.111	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
106.184.3.122	Japan	147.237.77.226	www.chamatz.aka.idf.il	Malformed URL	Block	1
66.249.78.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/smalim/showbig.aspx	Block	1
171.25.193.131	Sweden	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
105.137.65.133	Morocco	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.64.180	Israel	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
106.184.3.122	Japan	147.237.77.226	www.chamatz.aka.idf.il	Unknown HTTP Request Method SSH-2.0-LYGhost_1.2.7-20100630 in URL	Block	1
68.43.87.236	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
184.168.200.23	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1
105.137.65.133	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/c99.php	Block	1
66.249.64.185	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/links.aspx	Block	1
151.80.31.151	France	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9235-he/refuah.aspx	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/funeral.stm&lt	Block	1
5.39.222.159	Netherlands	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/rom-0	Block	1
198.58.103.91	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
106.38.241.149	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-13077-en/dovera93f95ecb7909e49	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1

04-20-2016-04:04:04 to 04-20-2016-05:04:04