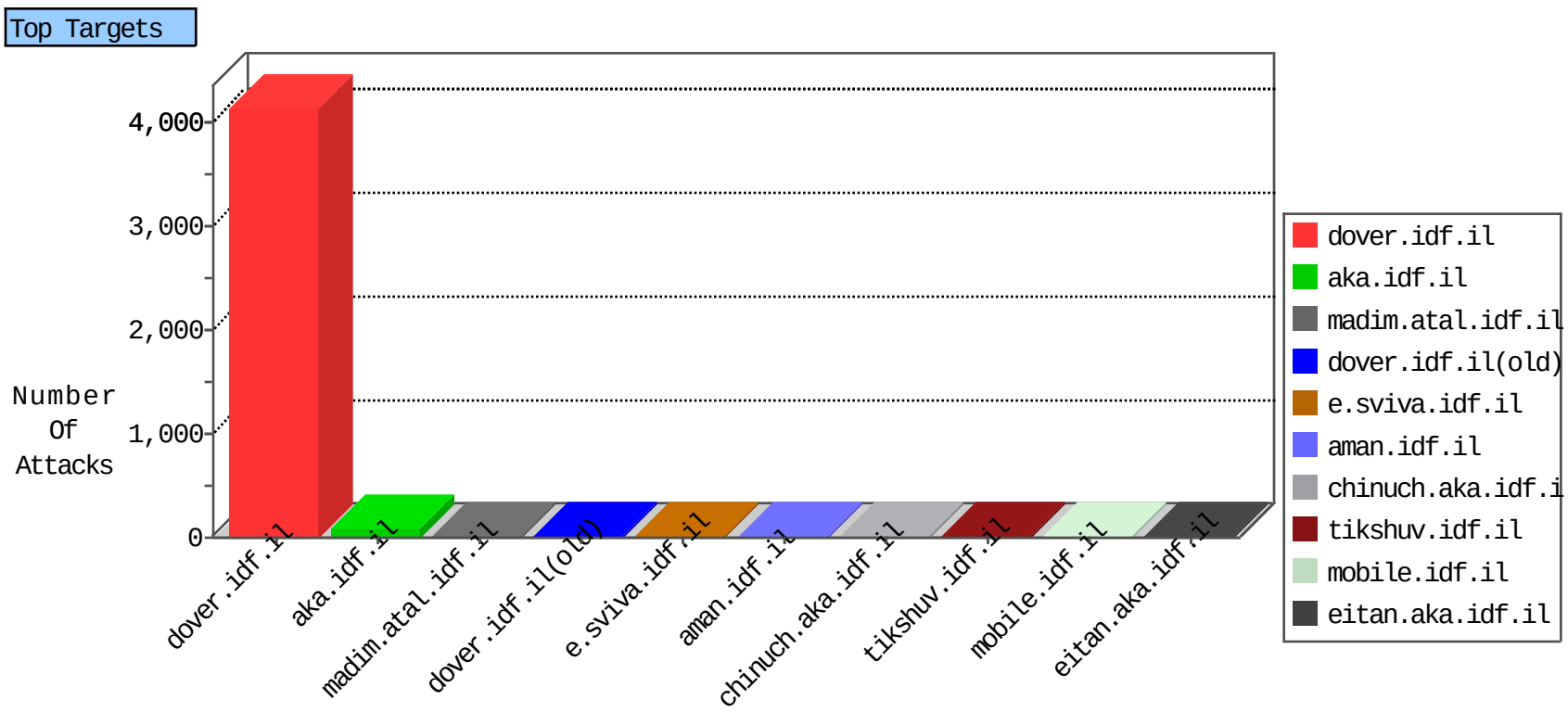
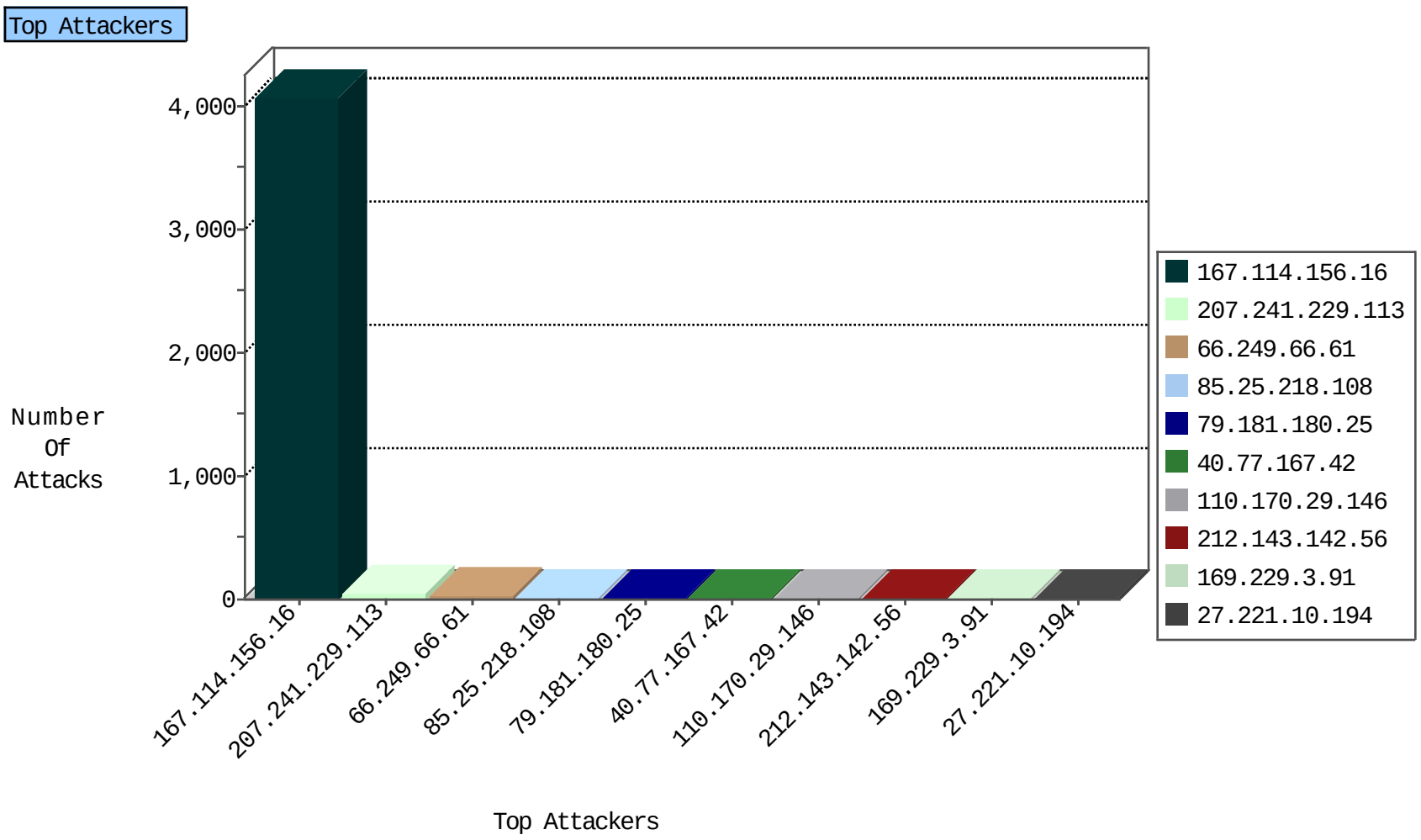
04-19-2016-04:04:00 to 04-19-2016-05:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-19-2016-04:04:00 to 04-19-2016-05:04:00

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	Block_Ip_Web_In	drop	4078
110.170.29.146	Thailand	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	7
85.25.218.108	Germany	147.237.72.14	dover.idf.il(old)	Block_Udp_All_Nets	drop	4
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
85.25.218.108	Germany	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	2
85.25.218.108	Germany	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	2
85.25.218.108	Germany	147.237.77.61	e.cogat.idf.il	Block_Udp_All_Nets	drop	2
68.180.230.184	United States	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	1
185.56.28.67	Netherlands	147.237.72.166	aka.idf.il	Block_Ntp_All_Net	drop	1
85.25.218.108	Germany	147.237.77.121	e.navy.idf.il	Block_Udp_All_Nets	drop	1
23.252.166.91	United States	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1

04-19-2016-04:04:00 to 04-19-2016-05:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-19-2016-04:04:00 to 04-19-2016-05:04:00

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
115.28.247.220	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
106.186.31.135	147.237.8.50	Japan	e.tikshuv.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
80.82.64.146	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
27.221.10.194	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
27.221.10.194	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
195.216.176.244	147.237.76.148	Latvia	gqcenter.aka.idf.i	ET SCAN NMAP -sS window 1024	1
194.126.22.222	147.237.0.19	Lebanon	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
183.60.48.25	147.237.0.15	China	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
113.240.250.154	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
106.184.2.29	147.237.76.31	Japan	nakchal.idf.il	ET SCAN Potential SSH Scan	1
27.221.10.194	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
27.221.10.194	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
185.106.92.47	147.237.76.198	Russian Federation	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1

04-19-2016-04:04:00 to 04-19-2016-05:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
207.241.229.113	United States	147.237.72.166	aka.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	39
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
79.181.180.25	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
40.77.167.42	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
5.255.253.51	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
50.240.82.133	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
69.139.5.135	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
79.181.101.42	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
100.2.12.213	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
79.181.101.42	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
141.212.122.209	United States	147.237.76.200	eitan.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
216.218.206.86	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.20	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.10.99.203	Switzerland	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
149.202.98.161	France	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
106.186.113.132	Japan	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
169.229.3.91	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.212	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
94.242.222.23	Luxembourg	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
216.218.206.86	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.60	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
176.10.104.240	Switzerland	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
46.119.127.129	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
158.255.5.147	Russian Federation	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.186.113.132	Japan	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.108.32.116	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
208.100.26.230	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
69.139.5.135	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	1
141.212.122.213	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
100.2.12.213	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
79.172.193.32	Hungary	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
184.105.139.84	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.120.191.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
109.201.152.227	Netherlands	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
89.31.96.168	Netherlands	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
169.229.3.91	United States	147.237.77.243	mobile.idf.il	drop	SAM rule	drop	1
141.212.122.219	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
100.2.12.213	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.227	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.120.191.13	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	drop	SAM rule	drop	1
141.212.122.208	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
92.222.103.234	France	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
216.218.206.80	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.10	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
171.25.193.78	Sweden	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1

04-19-2016-04:04:00 to 04-19-2016-05:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
157.55.39.171	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.85.249	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	3
219.74.37.168	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.66.101	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
207.46.13.53	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
94.242.222.23	Luxembourg	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
173.63.109.202	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
208.100.26.230	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
104.128.144.131	Canada	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/redirect.php	Block	1
198.58.102.158	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
66.249.66.176	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/robots.txt	Block	1
109.201.152.227	Netherlands	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
203.127.96.205	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
119.73.253.5	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
203.127.96.252	Singapore	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.230.184	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1238-he/atal.aspx	Block	1

04-19-2016-04:04:00 to 04-19-2016-05:04:00