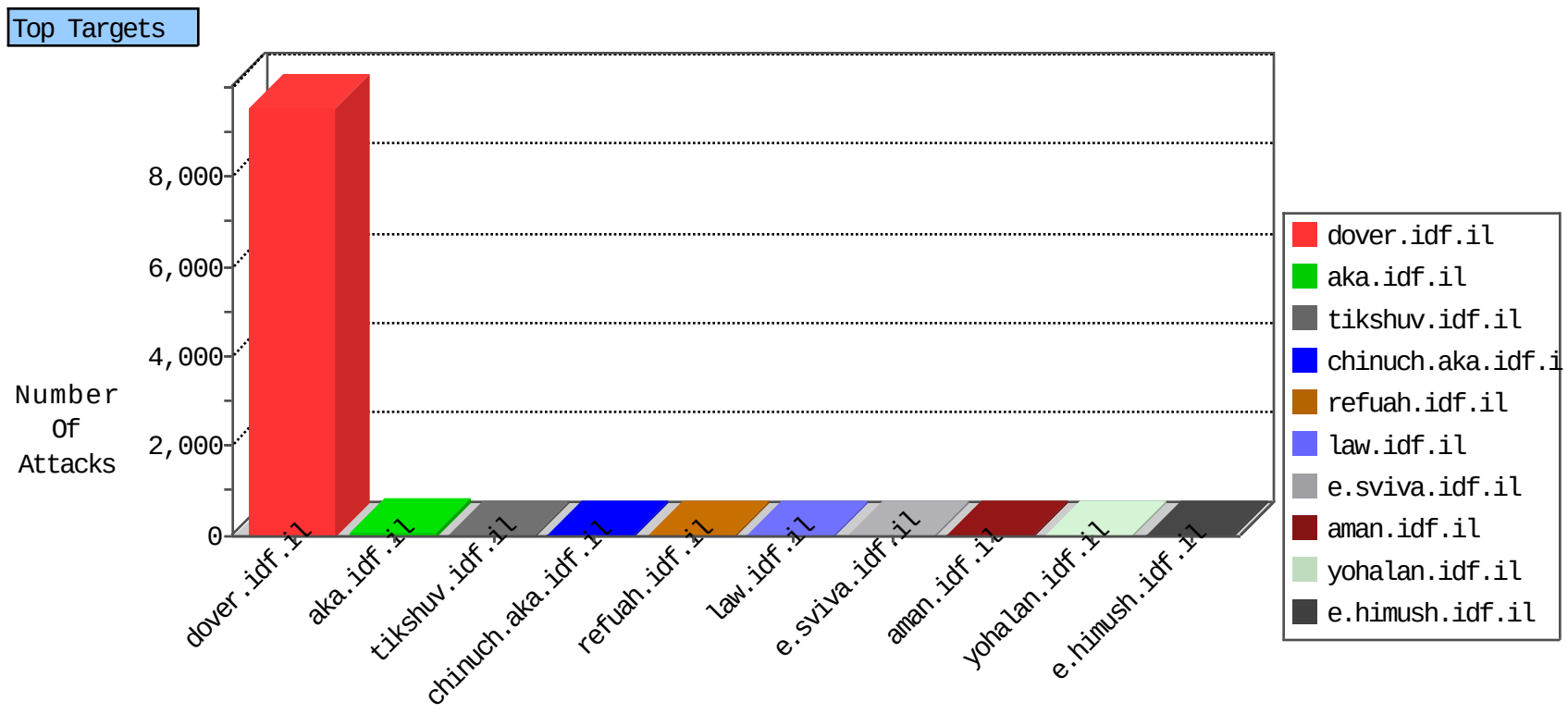
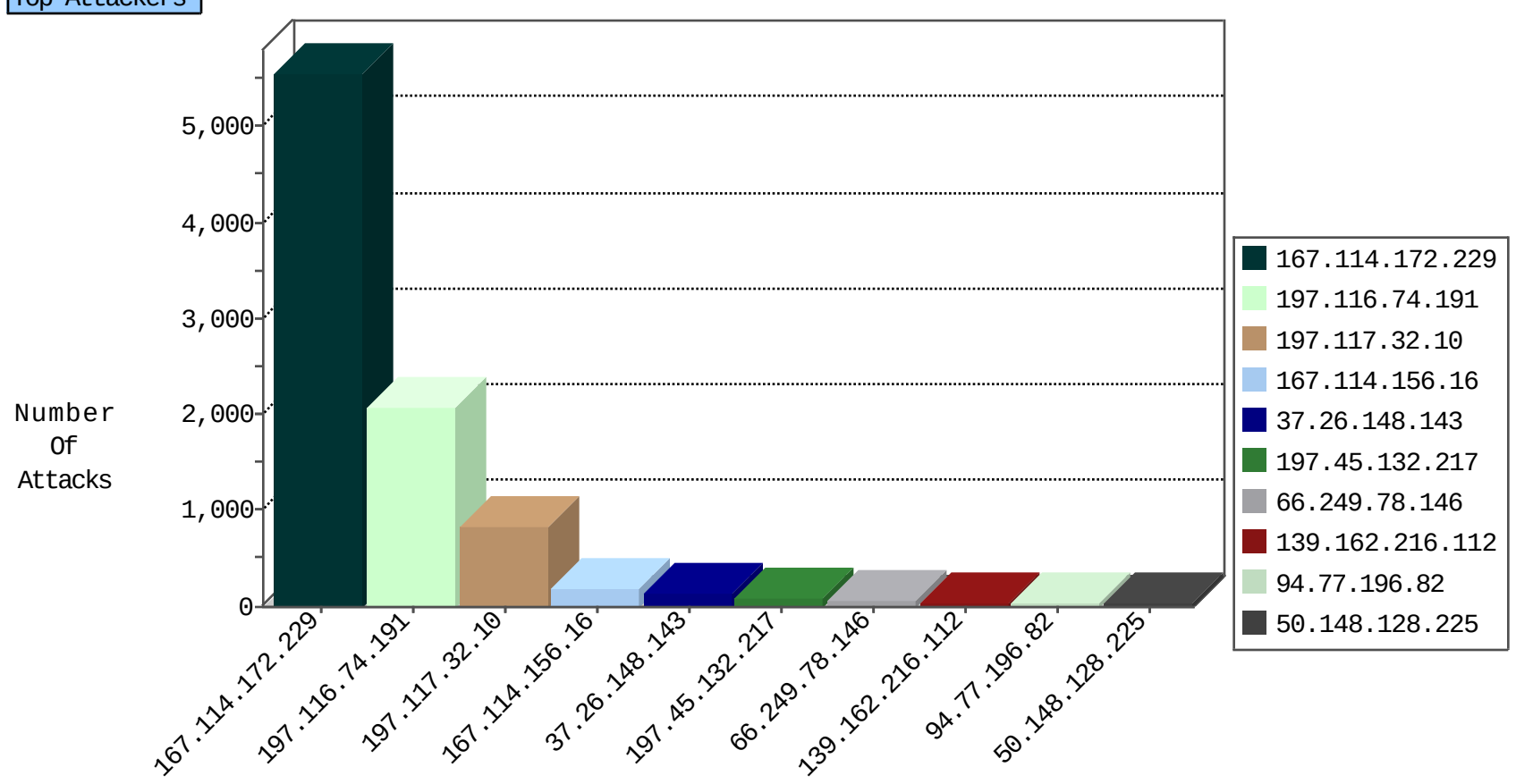
04-27-2016-04:04:09 to 04-27-2016-05:04:09

IDF Under Attack
Daily Report

Top Targets



Top Attackers



04-27-2016-04:04:09 to 04-27-2016-05:04:09

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	HTTP-POST-Segmented-DoS	dest-reset	9154
0.0.0.0		147.237.77.216	dover.idf.il	HTTP-POST-Segmented-DoS	dest-reset	228
197.116.74.191	Algeria	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	47
197.117.32.10	Algeria	147.237.77.216	dover.idf.il	DOS-HTTP-fireflood	dest-reset	12
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
169.54.233.116	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
169.54.233.116	United States	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
169.54.233.116	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
169.54.233.116	United States	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
94.102.49.116	Netherlands	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
197.117.32.10	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
169.54.233.116	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
169.54.233.116	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1
169.54.233.116	United States	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
204.42.253.2	United States	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
185.35.62.78	Switzerland	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
169.54.233.116	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
197.116.74.191	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
169.54.233.116	United States	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
185.35.62.130	Switzerland	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1

04-27-2016-04:04:09 to 04-27-2016-05:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.1.90.117	United States	147.237.77.216	dover.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

04-27-2016-04:04:09 to 04-27-2016-05:04:09

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
66.249.66.118	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sA (2)	2
201.175.93.101	147.237.77.74	Mexico	law.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
186.207.99.140	147.237.0.35	Brazil	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.82.106.200	147.237.72.14	India	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
163.172.140.23	147.237.77.178	United Kingdom	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.140.23	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
95.211.174.171	147.237.0.16	Netherlands	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.0.200	Ukraine	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
13.92.178.142	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1
201.175.93.101	147.237.77.234	Mexico	halag.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
13.92.103.193	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 4096	1
183.82.106.200	147.237.72.14	India	dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1
183.82.106.200	147.237.72.14	India	dover.idf.il(old)	ET SCAN NMAP -f -sS	1
163.172.140.23	147.237.76.34	United Kingdom	yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.140.23	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.0.200	Ukraine	m4u.idf.il	ET SCAN NMAP -sS window 3072	1
13.92.178.142	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 3072	1

04-27-2016-04:04:09 to 04-27-2016-05:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.172.229	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5555
197.116.74.191	Algeria	147.237.77.216	dover.idf.il	drop		drop	1011
197.116.74.191	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	537
197.116.74.191	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	453
197.117.32.10	Algeria	147.237.77.216	dover.idf.il	drop		drop	371
197.117.32.10	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	271
197.117.32.10	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	160
37.26.148.143	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	142
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	99
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	40
50.148.128.225	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
70.208.72.2	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
199.204.248.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
178.63.55.202	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
40.77.167.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
197.116.74.191	Algeria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
207.46.13.49	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
207.46.13.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
40.77.167.31	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
128.68.15.69	Russian Federation	147.237.0.34	tikshuv.idf.i	drop	First packet isn't SYN	drop	12
198.58.102.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.158	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
198.58.103.91	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.103.115	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
197.116.74.191	Algeria	147.237.77.216	dover.idf.il	drop	Unexpected post SYN packet - RST or SYN expected	drop	11
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
162.243.104.237	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
197.116.74.191	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
128.242.249.11	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
52.68.136.185	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
106.38.241.149	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
197.117.32.10	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
5.9.94.207	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
60.241.91.107	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
63.143.118.82	Jamaica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
163.172.21.10	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4

04-27-2016-04:04:09 to 04-27-2016-05:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
50.148.128.225	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in tikshuv.idf.il/site/story.aspx	Block	1
163.172.21.10	United Kingdom	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/resources/styles/master	Block	1
167.114.172.229	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/homepage/piwik.php	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/unselecatble.aspx	Block	1
163.172.21.10	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/administrator/index.php	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/7/3397.jpg	Block	1
172.85.211.18	United States	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
164.132.161.73	Italy	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/homepage/asp	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/scriptresource.axd	Block	1
197.116.74.191	Algeria	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on 147.237.77.216/	Block	1
141.212.122.161	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to 147.237.77.19/	Block	1
40.77.167.8	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
167.114.172.229	Canada	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.230.45	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8956-he/refuah.aspx	Block	1
207.46.13.89	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
163.172.21.10	United Kingdom	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 163.172.21.10	Block	1
167.114.172.229	Canada	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 167.114.172.229	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1

04-27-2016-04:04:09 to 04-27-2016-05:04:09