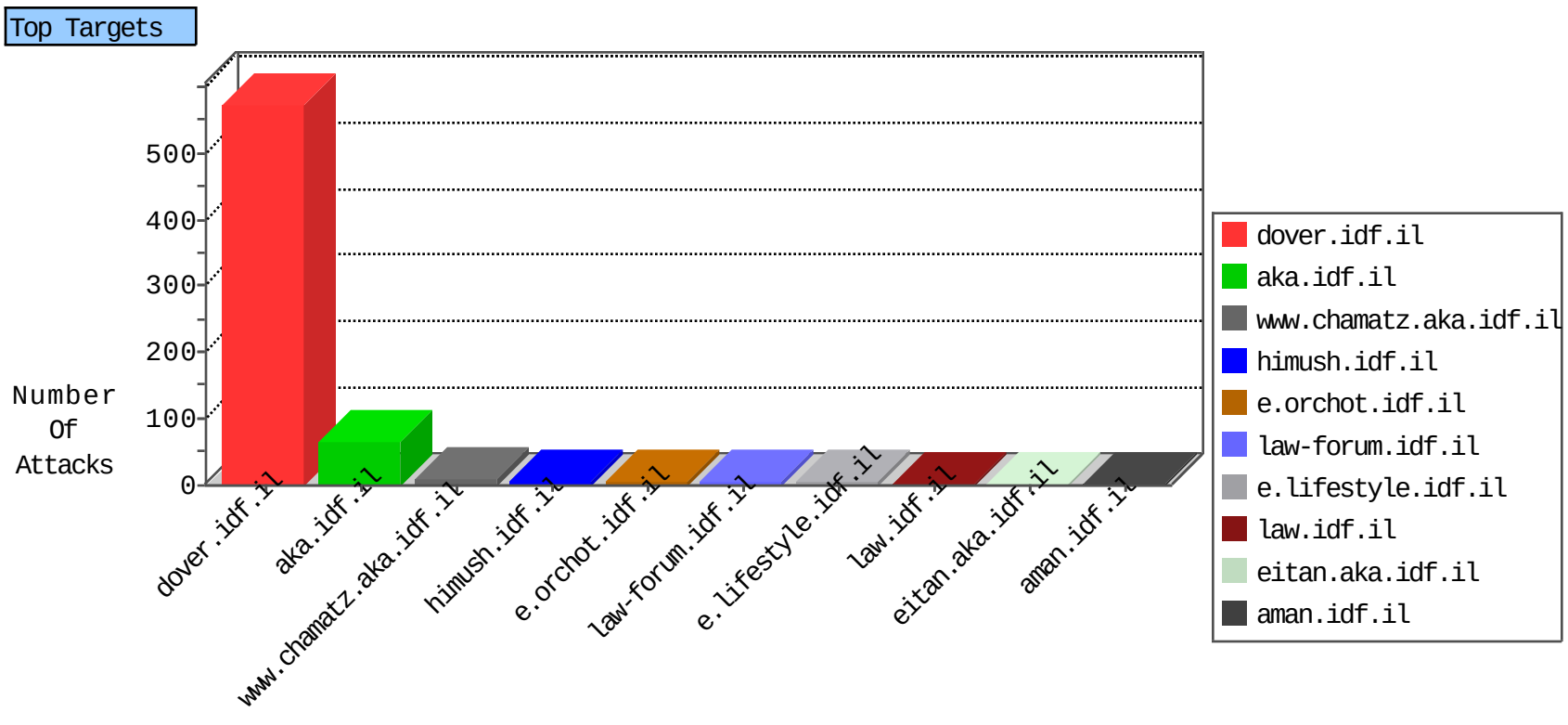
04-26-2016-04:04:04 to 04-26-2016-05:04:04

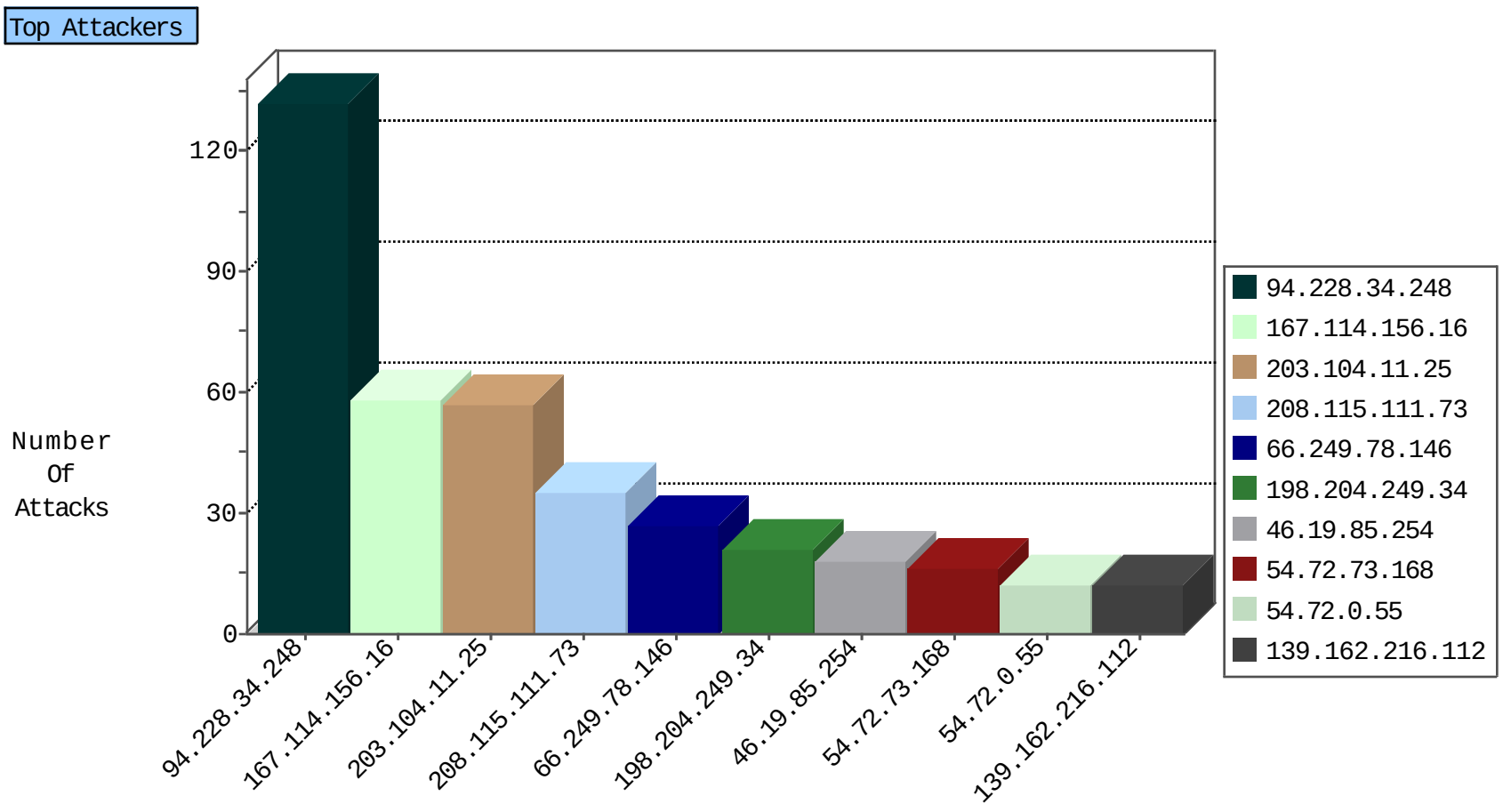
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

04-26-2016-04:04:04 to 04-26-2016-05:04:04

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	HTTP-POST-Segmented-DoS	dest-reset	2691
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	HTTP-MISC-Slowloris-DOS-Var1	dest-reset	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
45.63.20.231	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
204.42.253.130	United States	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
66.240.236.119	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
71.6.146.185	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
45.63.20.231	United States	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
71.6.165.200	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

04-26-2016-04:04:04 to 04-26-2016-05:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

04-26-2016-04:04:04 to 04-26-2016-05:04:04

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
202.29.86.129	147.237.77.235	Thailand	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
202.29.86.129	147.237.77.74	Thailand	law.idf.il	ET SCAN NMAP -sS window 1024	1
158.255.5.147	147.237.77.234	Russian Federation	halag.idf.il	ET SCAN NMAP -sS window 1024	1
158.255.5.147	147.237.0.16	Russian Federation	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
115.29.197.215	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
81.163.154.96	147.237.76.30	Ukraine	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
13.92.245.177	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 2048	1
202.29.86.129	147.237.77.243	Thailand	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
13.92.245.177	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -f -sS	1
202.29.86.129	147.237.77.216	Thailand	dover.idf.il	ET SCAN NMAP -sS window 1024	1
195.216.176.244	147.237.72.14	Latvia	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
193.227.34.78	147.237.77.235	Egypt	sviva.idf.il	ET SCAN NMAP -sS window 4096	1
158.255.5.147	147.237.0.19	Russian Federation	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
122.3.77.55	147.237.76.38	Philippines	e.e.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
107.6.130.113	147.237.0.33	United States	idf.il	ET SCAN Potential SSH Scan	1
80.82.78.38	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.230.74	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sS window 1024	1
13.92.245.177	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1

04-26-2016-04:04:04 to 04-26-2016-05:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
94.228.34.248	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	132
203.104.11.25	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	57
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
198.204.249.34	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
147.75.208.225	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
198.58.102.155	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
147.75.208.226	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
147.75.208.236	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
147.75.208.229	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
147.75.208.227	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
147.75.208.233	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
147.75.208.238	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
157.55.39.194	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
147.75.208.230	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
207.46.13.32	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.254	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
147.75.208.232	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
24.86.42.171	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
92.247.181.31	Bulgaria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
147.75.208.224	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
147.75.208.239	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
147.75.208.235	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
147.75.208.231	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
147.75.208.237	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
147.75.208.228	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
147.75.208.234	Switzerland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
141.8.142.33	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.30.78	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
157.55.39.74	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
119.93.157.77	Philippines	147.237.77.19	law-forum.idf.il	drop	First packet isn't SYN	drop	3
31.154.43.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.30.78	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
178.154.189.204	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.154.145.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.30.78	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
46.19.85.254	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
37.9.122.203	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.83.142	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.254	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
119.92.153.102	Philippines	147.237.76.30	himush.idf.il	drop	First packet isn't SYN	drop	3

04-26-2016-04:04:04 to 04-26-2016-05:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.235.65.236	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to kosher-kravi.idf.il/shared/usercontrols/headerupper/	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
41.105.41.254	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
157.55.39.246	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
72.73.252.232	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navydefault.aspx	Block	1
147.75.208.233	Switzerland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	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
176.13.14.85	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
77.75.76.172	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/33/	Block	1
147.75.208.237	Switzerland	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
67.19.79.218	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /robots.txt	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
84.95.208.20	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
31.154.43.65	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
157.55.39.132	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/2/62532.pdf	Block	1
68.180.229.241	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1927-he/cogat.aspx	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/main/giyus/general.aspx	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
41.105.41.254	Algeria	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
157.55.39.194	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1362-he/dover.aspx	Block	1

04-26-2016-04:04:04 to 04-26-2016-05:04:04