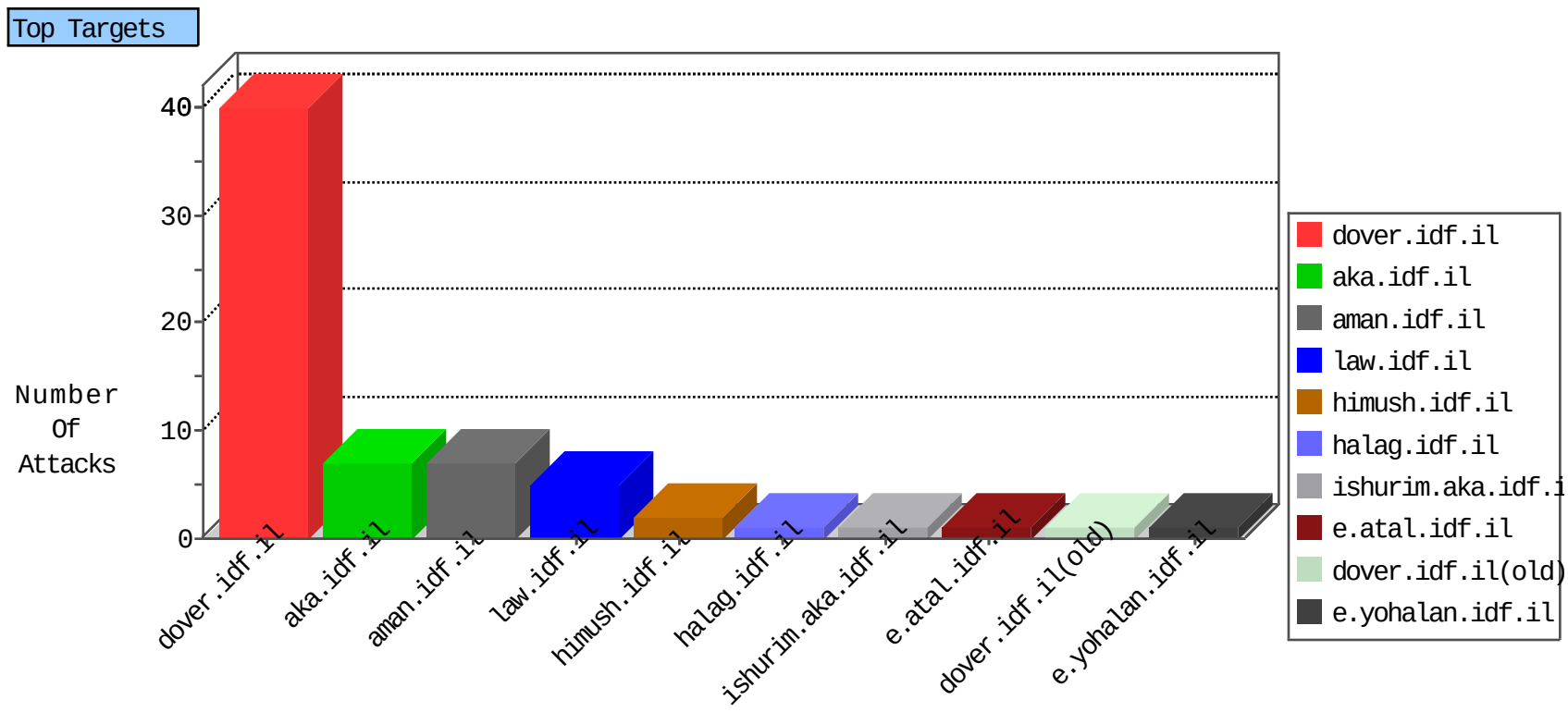
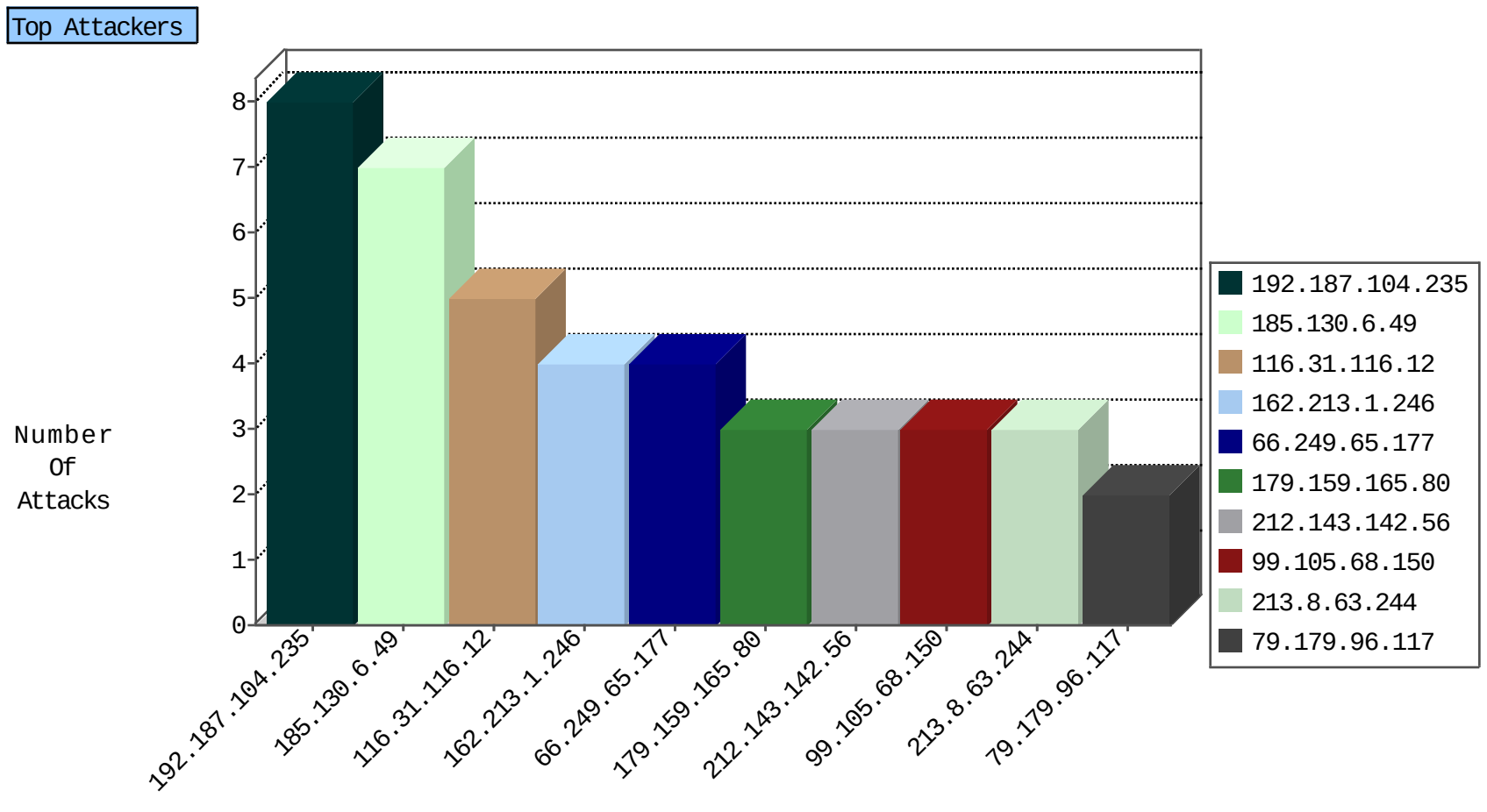
08-21-2016-06:04:02 to 08-21-2016-07:04:02

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-21-2016-06:04:02 to 08-21-2016-07:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.92.131.22	Ireland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
41.206.63.131	Kenya	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
196.200.16.202	Kenya	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
117.141.120.79	China	147.237.76.148	gqcenter.aka.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
185.92.131.23	Ireland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
41.206.63.132	Kenya	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
196.200.16.203	Kenya	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
185.92.131.20	Ireland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
185.92.131.24	Ireland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
41.206.63.133	Kenya	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
185.92.131.21	Ireland	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
41.206.63.130	Kenya	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
196.200.16.201	Kenya	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
82.80.78.2	Israel	147.237.77.216	dover.idf.il	Black List	drop	1

08-21-2016-06:04:02 to 08-21-2016-07:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.130.6.49	Lithuania	147.237.72.156	aman.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
192.187.104.235	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	4
192.187.104.235	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
192.187.104.235	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	2
185.94.116.30	United Kingdom	147.237.77.216	dover.idf.il	25004: HTTP: WordPress Pingback Redirect Request	Block	1
185.130.6.49	Lithuania	147.237.72.156	aman.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
164.132.161.6	Italy	147.237.76.147	chinuch.aka.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

08-21-2016-06:04:02 to 08-21-2016-07:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
162.213.1.246	147.237.77.216	United States	dover.idf.il	Tehila - Perl LWP with fake user agent	4
99.105.68.150	147.237.72.166	United States	aka.idf.il	ET SCAN Potential SSH Scan	2
46.120.122.219	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	1
185.130.6.49	147.237.72.156	Lithuania	aman.idf.il	ET WEB_SERVER Muieblackcat scanner	1
123.206.85.139	147.237.8.14	China	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
116.31.116.12	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
116.31.116.12	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
82.166.91.92	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	1
65.156.199.242	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.204.245	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
36.72.242.87	147.237.76.31	Indonesia	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
116.31.116.12	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
116.31.116.12	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
116.31.116.12	147.237.0.15	China	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
99.105.68.150	147.237.72.14	United States	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
66.249.66.242	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
58.218.204.245	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1

08-21-2016-06:04:02 to 08-21-2016-07:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
213.8.63.244	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
179.159.165.80	Brazil	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
199.58.86.209	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2

08-21-2016-06:04:02 to 08-21-2016-07:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.65.177	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.177	Block	3
71.6.158.166	United States	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/robots.txt	Block	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
66.249.65.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
75.82.117.252	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	1
66.249.76.31	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1681	Block	1
79.179.96.117	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.76.112	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
79.179.96.117	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
66.240.192.138	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/robots.txt	Block	1
66.249.79.139	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/ui/i18n/jquery-ui-i18n.js	Block	1
157.55.39.110	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1

08-21-2016-06:04:02 to 08-21-2016-07:04:02