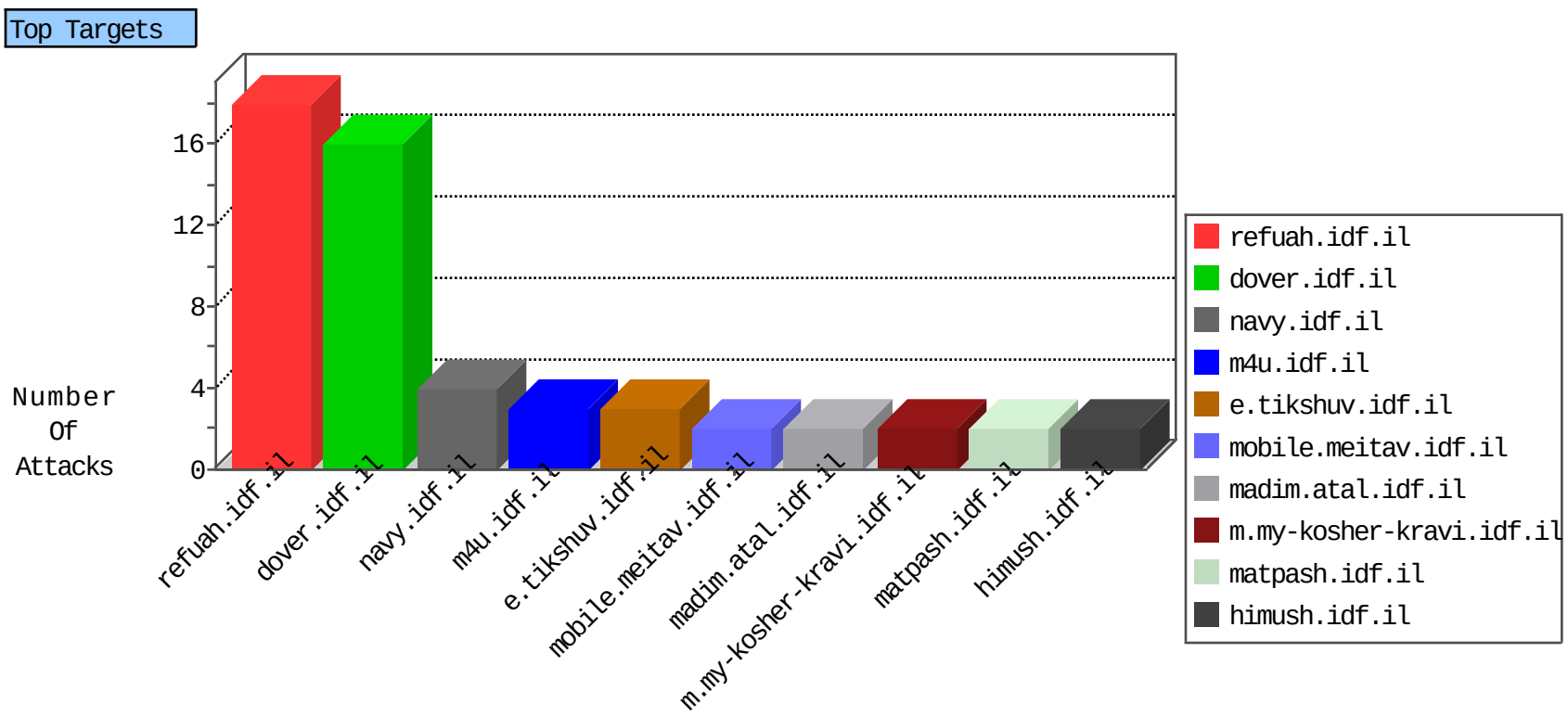
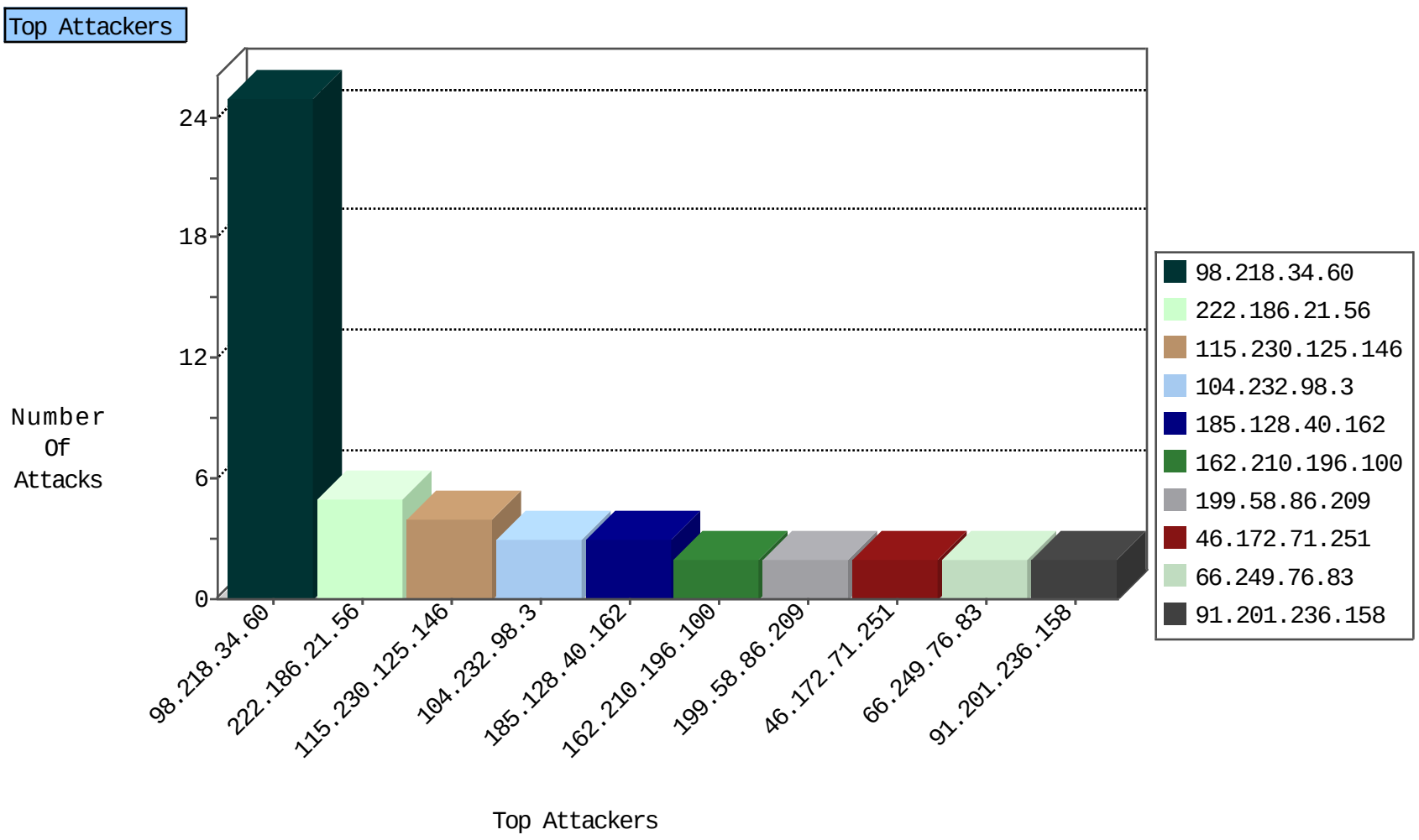
08-20-2016-08:04:06 to 08-20-2016-09:04:06

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-20-2016-08:04:06 to 08-20-2016-09:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.128.40.162	Switzerland	147.237.76.30	himush.idf.il	Black List	drop	1
222.186.21.56	China	147.237.76.39	mobile.meitav.idf.il	JLM_Under_Attack_Con_Http	drop	1
115.230.125.146	China	147.237.77.61	e.cogat.idf.il	JLM_Purple_Con_Limit_Http	drop	1
185.128.40.162	Switzerland	147.237.76.86	navy.idf.il	Black List	drop	1
115.230.125.146	China	147.237.77.74	law.idf.il	JLM_Purple_Con_Limit_Http	drop	1
185.128.40.162	Switzerland	147.237.76.196	e.sviva.idf.il	Black List	drop	1
115.230.125.146	China	147.237.77.179	e.mazi.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
222.186.21.56	China	147.237.76.39	mobile.meitav.idf.il	JLM_Purple_Con_Limit_Http	drop	1

08-20-2016-08:04:06 to 08-20-2016-09:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
98.218.34.60	United States	147.237.76.42	refuah.idf.il	C1000074: HTTP: majestic bot	Permit	17
98.218.34.60	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	6
162.210.196.100	United States	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Permit	2
199.58.86.209	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
98.218.34.60	United States	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Permit	2
71.6.165.200	United States	147.237.8.14	e.orchot.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

08-20-2016-08:04:06 to 08-20-2016-09:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.201.236.158	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
71.6.167.142	147.237.8.45	United States	e.eitan.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
222.186.21.56	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
50.84.213.146	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 3072	1
216.81.230.167	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 1024	1
46.172.71.251	147.237.76.34	Ukraine	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
180.97.81.71	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
114.32.20.3	147.237.76.30	Taiwan	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.232.98.3	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
95.211.129.27	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
79.140.10.43	147.237.76.31	Ukraine	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
222.186.21.56	147.237.77.205	China	prisha.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.163.35.221	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.56	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.172.71.251	147.237.76.147	Ukraine	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
191.96.249.231	147.237.0.200	Chile	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
179.43.141.228	147.237.8.27	Switzerland	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
104.232.98.3	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 3072	1
104.232.98.3	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -f -sS	1
94.102.48.195	147.237.72.156	Netherlands	aman.idf.il	ET SCAN NMAP -sS window 1024	1

08-20-2016-08:04:06 to 08-20-2016-09:04:06

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	1
31.13.97.100	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
31.13.97.103	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
115.230.125.146	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
163.53.75.10	India	147.237.0.200	m4u.idf.il	drop		drop	1

08-20-2016-08:04:06 to 08-20-2016-09:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.76.83	Israel	147.237.77.216	dover.idf.i	Multiple Unauthorized URL Access from 66.249.76.83	Block	2
87.69.191.155	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1501-he/atal.aspx	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.i	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
199.30.24.177	United States	147.237.77.216	dover.idf.i	Unauthorized URL Access to www.idf.il/error.htm	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
77.138.154.92	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/rights/asp/info.asp	Block	1

08-20-2016-08:04:06 to 08-20-2016-09:04:06