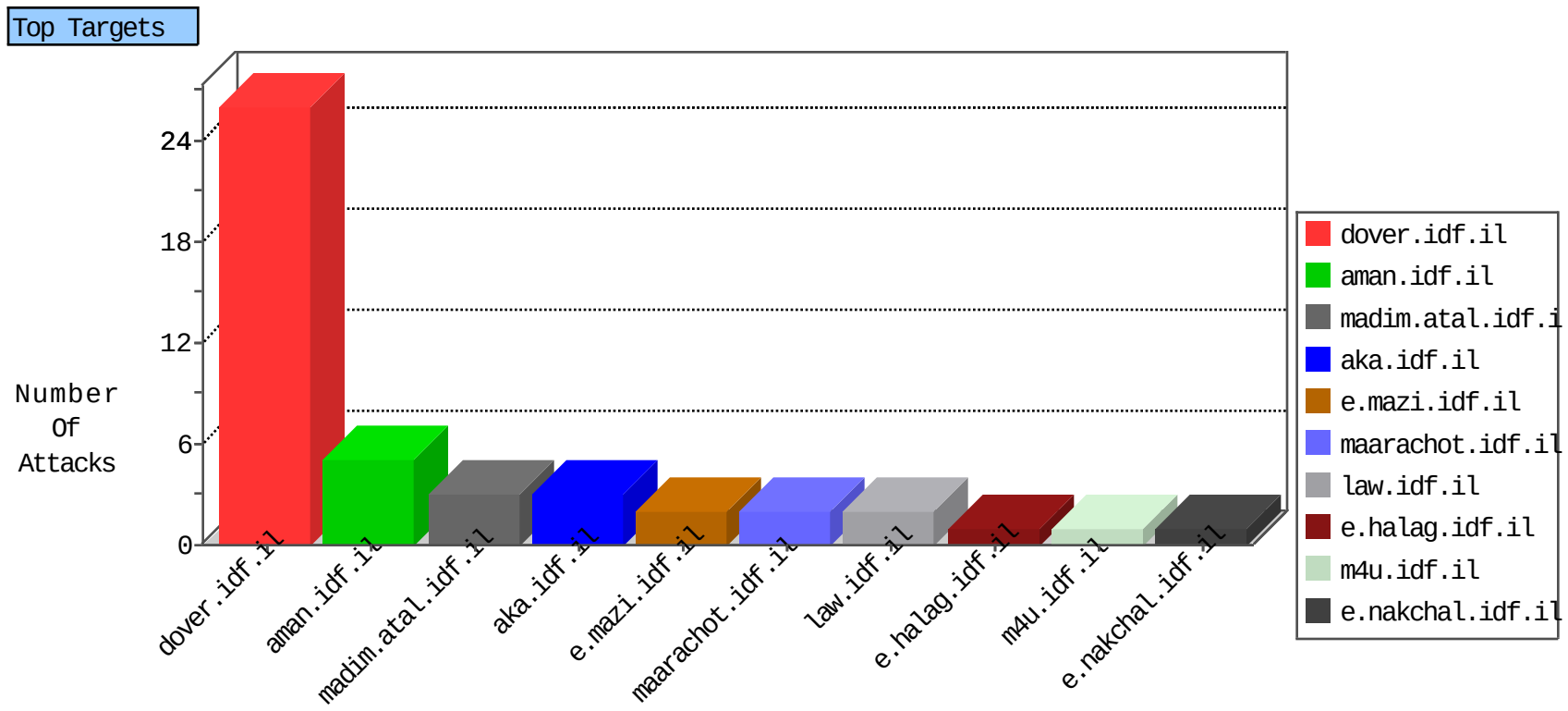
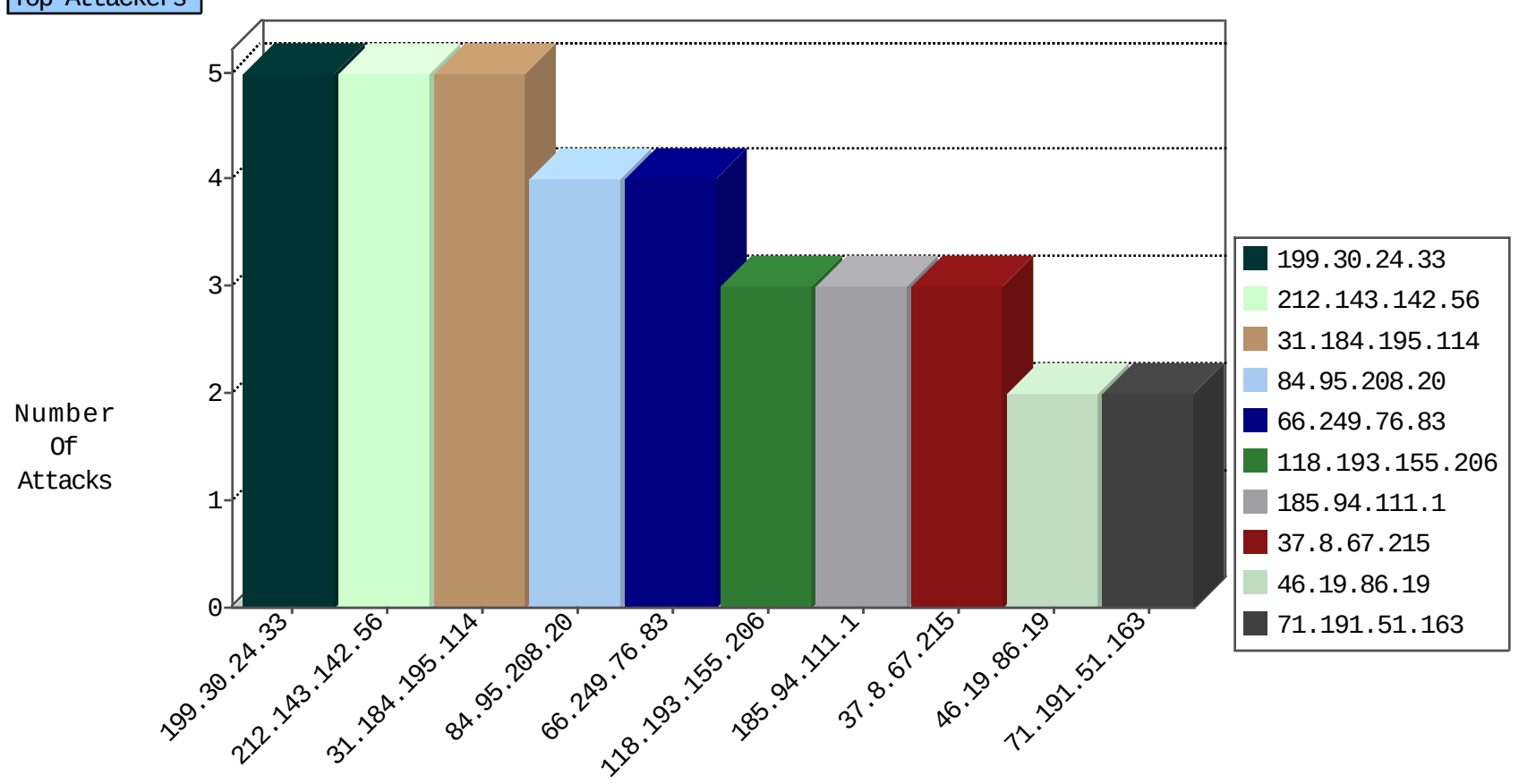
08-20-2016-01:05:26 to 08-20-2016-02:05:26

IDF Under Attack Daily Report

Top Targets



Top Attackers



08-20-2016-01:05:26 to 08-20-2016-02:05:26

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
185.94.111.1	Russian Federation	147.237.76.42	refuah.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.44	e.refuah.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
115.230.125.146	China	147.237.76.202	e.halag.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
195.154.172.204	France	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Http	drop	1

08-20-2016-01:05:26 to 08-20-2016-02:05:26

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
118.193.155.206	China	147.237.77.216	dover.idf.il	C1000016: HTTP: administrator in URI	Permit	1
80.181.111.140	Italy	147.237.8.14	e.orchot.idf.il	12890: TCP: Windows TCP/IP Denial-of-Service Vulnerability (ONLY enable when under DoS attack)	Block	1
80.181.111.140	Italy	147.237.8.28	e.mobile-ks.idf.i	12890: TCP: Windows TCP/IP Denial-of-Service Vulnerability (ONLY enable when under DoS attack)	Block	1

08-20-2016-01:05:26 to 08-20-2016-02:05:26

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
190.8.169.58	147.237.77.170	Venezuela	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.77.176	Ukraine	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
50.84.213.146	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
31.184.195.114	147.237.77.121	Russian Federation	e.navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
31.184.195.114	147.237.76.39	Russian Federation	mobile.meitav.idf.i	ET SCAN Potential VNC Scan 5900-5920	1
31.184.195.114	147.237.0.35	Russian Federation	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
190.8.169.58	147.237.77.170	Venezuela	maarachot.idf.il	ET SCAN NMAP -sS window 4096	1
94.102.48.195	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
50.84.213.146	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
41.228.33.162	147.237.77.74	Tunisia	law.idf.il	ET SCAN NMAP -sS window 1024	1
31.184.195.114	147.237.76.177	Russian Federation	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
31.184.195.114	147.237.76.31	Russian Federation	nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.86.123.170	147.237.0.19	China	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1

08-20-2016-01:05:26 to 08-20-2016-02:05:26

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	5
37.8.67.215	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
195.154.172.204	France	147.237.0.33	idf.il	drop		drop	1
156.199.8.19	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1

08-20-2016-01:05:26 to 08-20-2016-02:05:26

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.30.24.33	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.76.83	Block	2
46.19.86.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.76.83	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	2
84.95.208.20	Israel	147.237.72.156	aman.idf.il	PHP Attempt	Block	1
66.249.66.242	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/228-he/faq.aspx	Block	1
71.191.51.163	United States	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtEmail in www.idf.il/1038-en/dover.aspx	Block	1
95.210.119.112	Europe	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
84.95.208.20	Israel	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to www.kosher-kravi.idf.il/default.aspx	Block	1
105.107.64.213	Algeria	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/robots.txt	Block	1
46.229.164.102	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
118.193.155.206	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.76.106	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/giyus/[[#11]]general.aspx	Block	1
84.95.208.20	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.102.9.43	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
118.193.155.206	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
71.191.51.163	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1

08-20-2016-01:05:26 to 08-20-2016-02:05:26