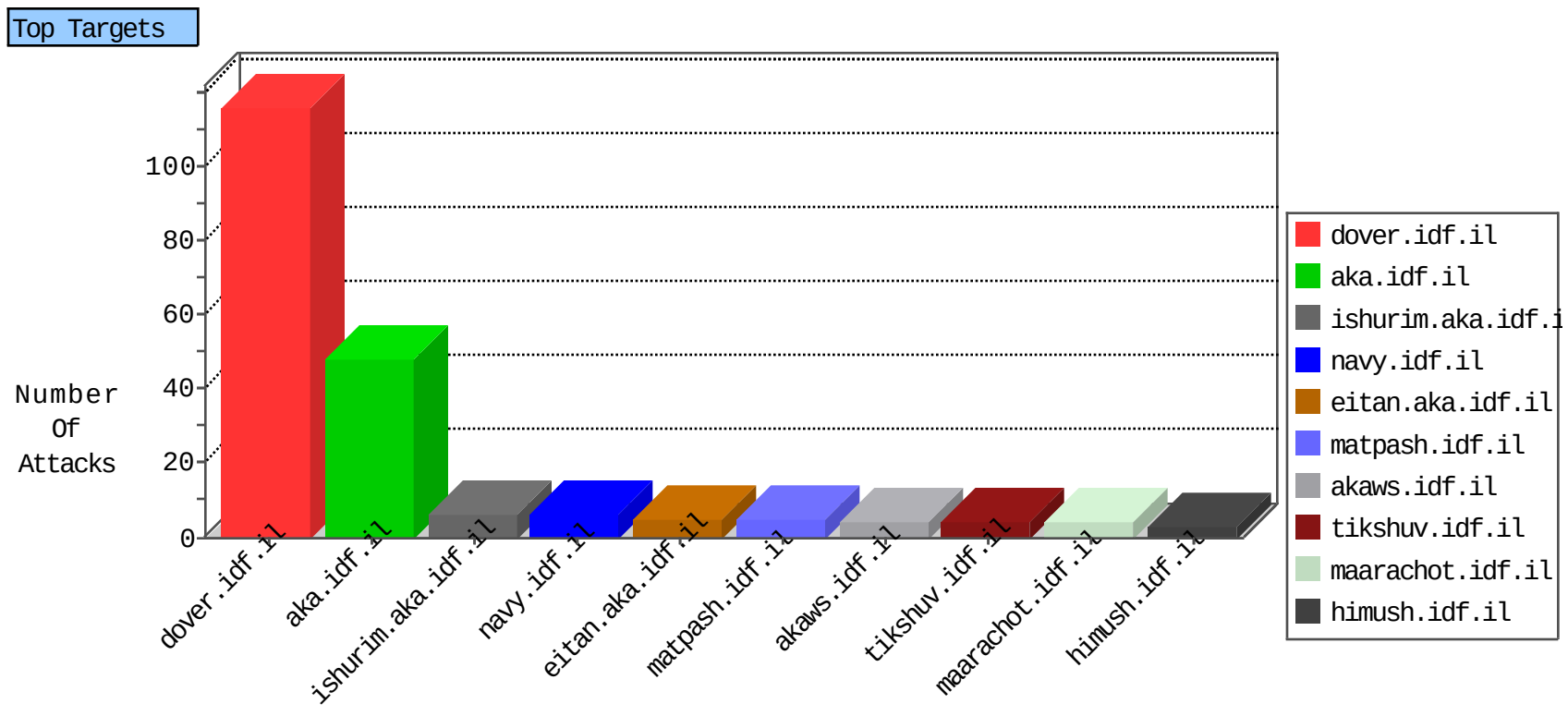
02-17-2016-03:04:05 to 02-17-2016-04:04:05

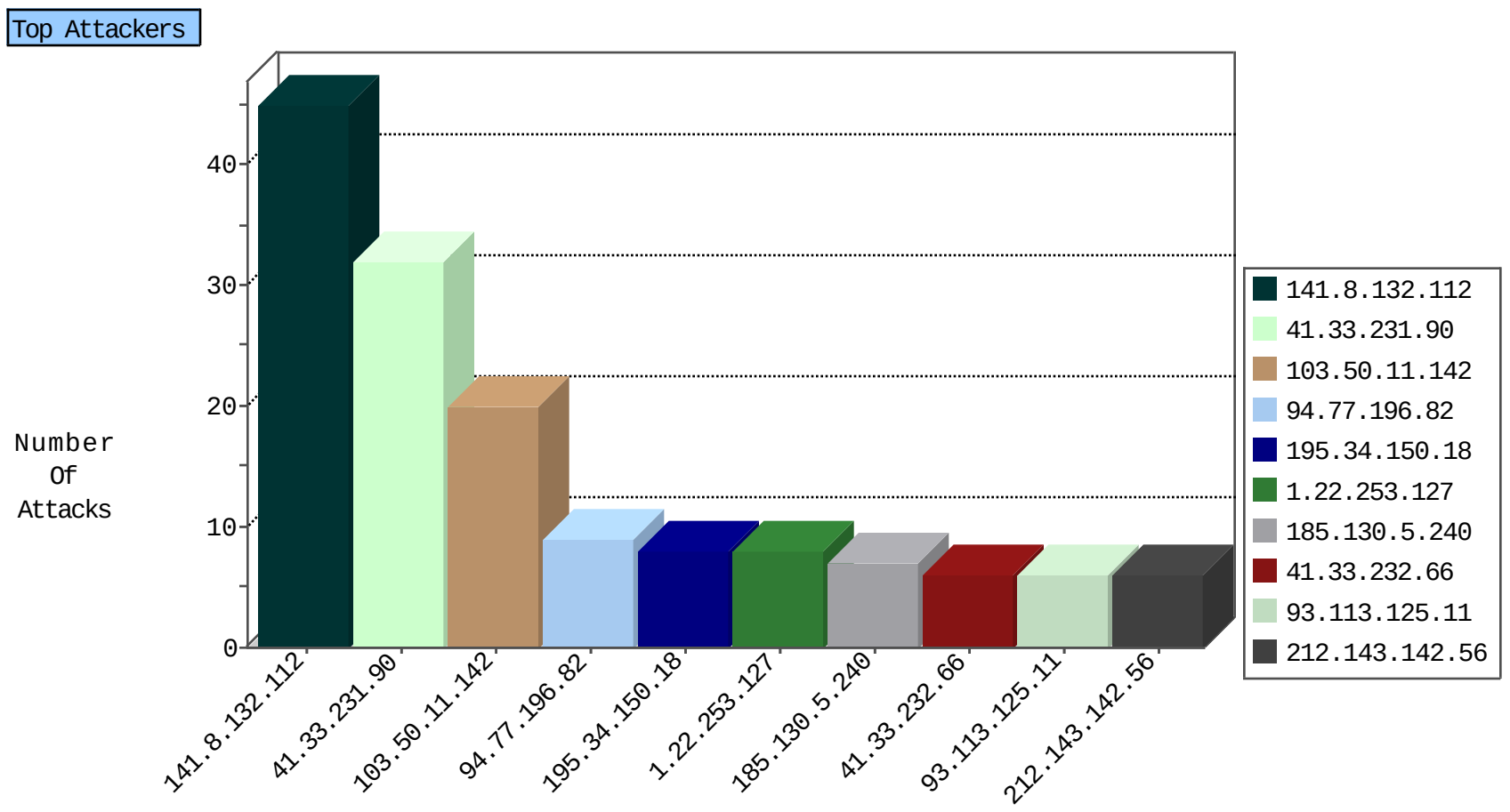
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-17-2016-03:04:05 to 02-17-2016-04:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.94.111.1		147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
162.248.100.195	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
185.35.62.71	Switzerland	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
69.195.146.78	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
185.35.62.147	Switzerland	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
71.6.165.200	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1

02-17-2016-03:04:05 to 02-17-2016-04:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-17-2016-03:04:05 to 02-17-2016-04:04:05

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
66.102.7.129	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	2
185.130.5.240	147.237.76.177		ncore.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.240	147.237.76.147		chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.240	147.237.0.34		tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
175.110.116.250	147.237.76.30	Pakistan	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
218.246.0.97	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
189.220.24.167	147.237.0.34	Mexico	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.130.5.240	147.237.77.178		e.matpash.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.130.5.240	147.237.76.147		chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.130.5.240	147.237.0.35		akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.130.5.240	147.237.0.16		my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.0.35	China	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.48.193	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
189.220.24.167	147.237.0.15	Mexico	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

02-17-2016-03:04:05 to 02-17-2016-04:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	45
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
103.50.11.142		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
74.73.166.84	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
199.30.16.179	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
93.113.125.11	Romania	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	3
192.185.4.108	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
136.243.67.234	Germany	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
108.167.133.30	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
131.253.24.132	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
81.169.237.146	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	1
41.207.17.110	Cote D'Ivoire	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
141.212.122.184	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
65.55.218.34	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.189	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
81.169.237.146	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	1
46.19.85.76	Israel	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.185	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
65.55.218.52	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.88	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.205	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
136.243.67.234	Germany	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
93.113.125.11	Romania	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
195.251.203.200	Greece	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.187	United States	147.237.0.35	akaws.idf.il	drop		drop	1
141.212.122.206	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
137.116.71.170	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
93.113.125.11	Romania	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
141.212.122.188	United States	147.237.0.35	akaws.idf.il	drop		drop	1
128.242.249.12	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
81.169.237.146	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	1
157.55.39.154	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.188	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

02-17-2016-03:04:05 to 02-17-2016-04:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
1.22.253.127	India	147.237.77.216	dover.idf.il	PHP Attempt	Block	4
1.22.253.127	India	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	4
153.107.192.206	Australia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	2
153.107.193.212	Australia	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.64.239	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1247-he/atal.aspx	Block	1
207.46.13.153	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-12967-he/dover.aspx	Block	1
41.207.17.110	Cote D'Ivoire	147.237.77.216	dover.idf.il	eMail Hoarding	Block	1
157.55.39.88	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to www.maarachot.idf.il/pdf/files/Ã~â€™Ã~â„¢Ã—Å“Ã—â„¢Ã—â€¢Ã—Â Ã—â€¢Ã—Âª	Block	1
66.249.66.67	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/4/108124.pdf	Block	1
208.115.111.73	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/miluim/templates/www.behazdaa.org	Block	1
68.180.228.162	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/1105-en/contactus.aspx	Block	1
66.249.64.166	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/938-he/nakhal.aspx	Block	1
157.55.39.94	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/igf	Block	1
66.249.66.125	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/sip_storage/files/4/1604.pdf	Block	1
93.113.125.11	Romania	147.237.72.167	ishurim.aka.idf.i	Unauthorized URL Access to /	Block	1
66.249.64.170	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
66.249.66.126	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/4/105564.pdf	Block	1
66.249.64.234	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
200.83.101.18	Chile	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	1
41.207.17.110	Cote D'Ivoire	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1

02-17-2016-03:04:05 to 02-17-2016-04:04:05