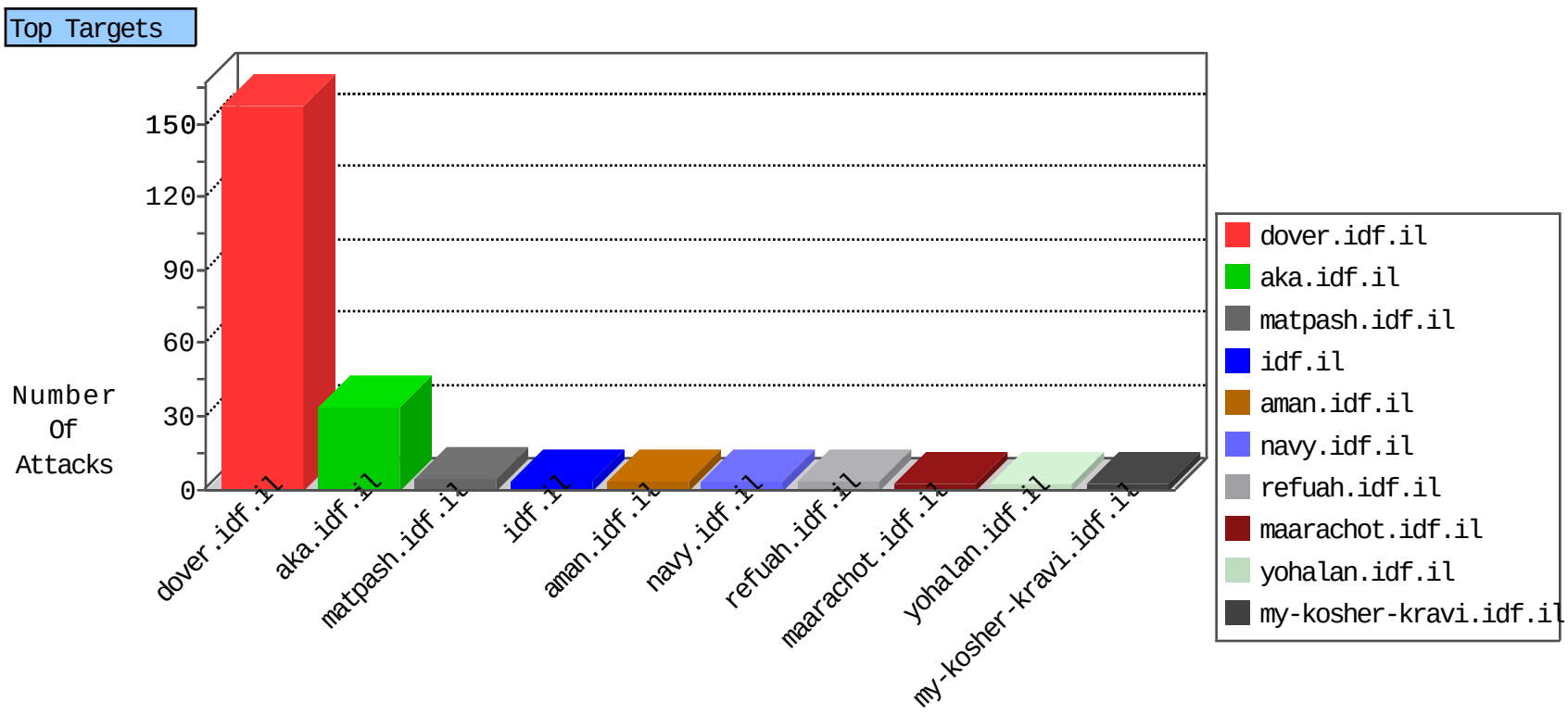
02-26-2016-05:04:08 to 02-26-2016-06:04:08

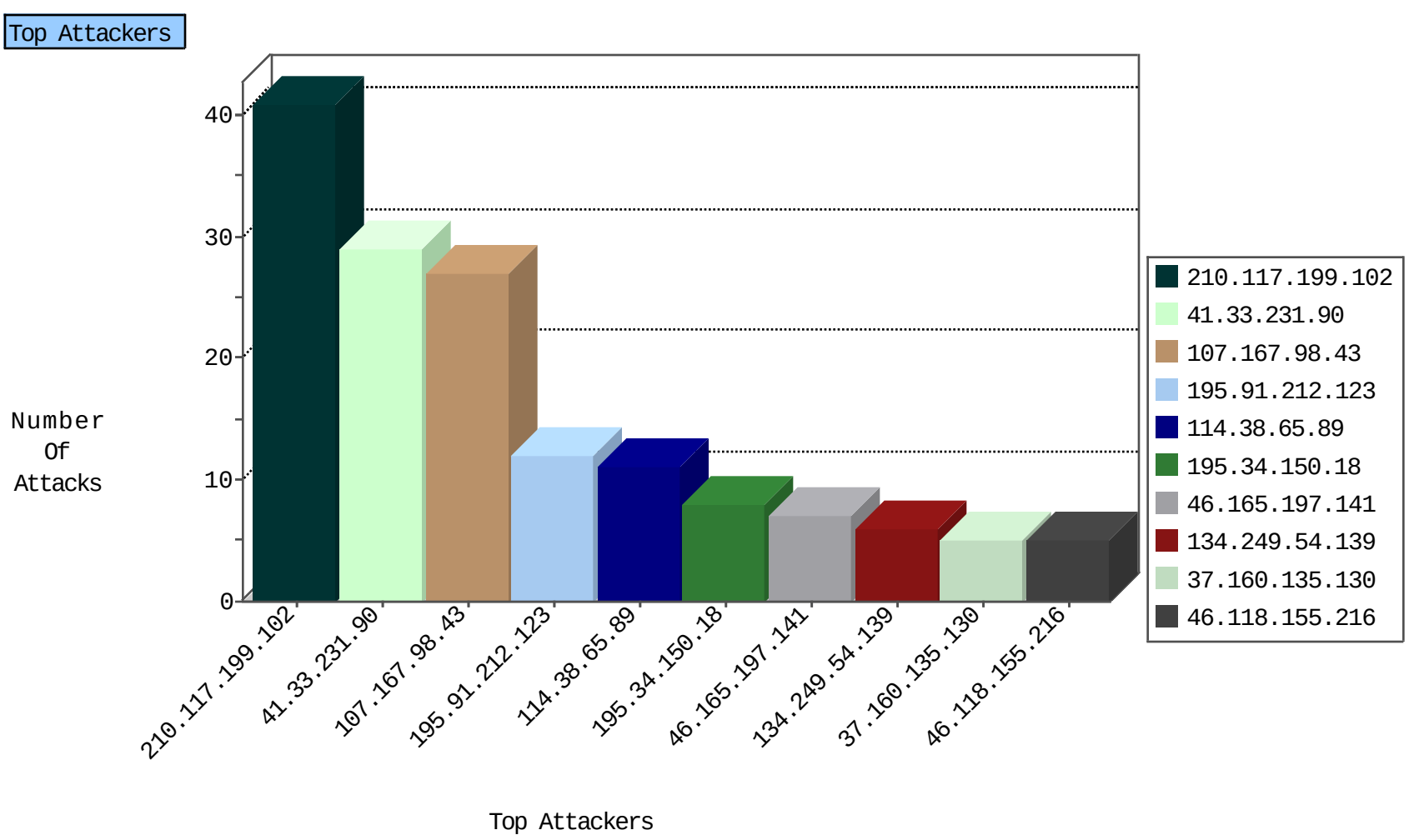
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-26-2016-05:04:08 to 02-26-2016-06:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
208.100.26.228	United States	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	1
208.100.26.228	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1

02-26-2016-05:04:08 to 02-26-2016-06:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
62.210.143.245	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
176.9.131.69	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
188.165.15.44	France	147.237.72.156	aman.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
188.165.15.59	France	147.237.76.86	navy.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

02-26-2016-05:04:08 to 02-26-2016-06:04:08

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
185.130.5.173	147.237.0.33		idf.il	ET SCAN Potential VNC Scan 5900-5920	1
146.185.250.2	147.237.77.216	Russian Federation	dover.idf.il	ET SCAN Potential SSH Scan	1
120.55.90.163	147.237.76.198	China	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
91.230.110.131	147.237.72.166	Russian Federation	aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
62.210.142.238	147.237.76.34	France	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.173	147.237.0.35		akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
185.130.5.173	147.237.0.19		madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
146.185.250.2	147.237.77.121	Russian Federation	e.navy.idf.il	ET SCAN Potential SSH Scan	1
108.61.228.113	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
62.210.142.238	147.237.76.39	France	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
186.47.214.66	147.237.8.28	Ecuador	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

02-26-2016-05:04:08 to 02-26-2016-06:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	29
107.167.98.43	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	27
210.117.199.102	Korea, Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
210.117.199.102	Korea, Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	14
114.38.65.89	Taiwan	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.179.109.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.31.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.160.135.130	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.77.196.82	Saudi Arabia	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
46.165.197.141	Germany	147.237.76.86	navy.idf.il	drop	SAM rule	drop	2
46.165.197.141	Germany	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	2
46.165.197.141	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
188.50.196.90	Saudi Arabia	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
66.249.78.160	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
89.138.72.137	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.40	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.72	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.144	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
188.48.218.166	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
69.167.168.241	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
141.212.122.148	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.160.135.130	France	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.73	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
91.230.110.131	Russian Federation	147.237.72.166	aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
195.62.53.168	Russian Federation	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.44	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.111	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.145	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.98	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
85.65.3.7	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
188.48.218.166	Saudi Arabia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
71.6.135.131	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.157	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.74	United States	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
199.30.24.150	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.52	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.219	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.145	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.39.222.159	Netherlands	147.237.0.33	idf.il	drop		drop	1
114.38.65.89	Taiwan	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
216.218.206.98	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
85.65.3.7	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
188.50.196.90	Saudi Arabia	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	1
74.82.47.38	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.158	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.74	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
74.82.47.60	United States	147.237.76.34	yohalan.idf.il	drop		drop	1

02-26-2016-05:04:08 to 02-26-2016-06:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
195.91.212.123	Russian Federation	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
134.249.54.139	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi/	Block	6
195.91.212.123	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 195.91.212.123	Block	5
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 46.118.155.216	Block	3
78.40.177.35	Lebanon	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/favicon.ico	Block	1
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
178.255.87.242	United Kingdom	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/robots.txt	Block	1
66.249.78.51	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/3/111543.pdf	Block	1
91.230.110.131	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
50.162.186.231	United States	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
178.255.215.87	France	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.78.58	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
5.29.33.173	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl13 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
195.91.212.123	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
114.38.65.89	Taiwan	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/usercontrols/headerupper/	Block	1
66.249.64.51	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
184.157.12.211	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.78.236	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/imagevideogallerylobby/imagevideogallerylobby.js	Block	1
198.20.69.74	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/robots.txt	Block	1
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/templatecontrols/news/לכתבה המלאה	Block	1
66.249.64.56	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/webresource.axd	Block	1
185.118.27.15		147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
66.249.78.242	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/1.he/langstyle.css	Block	1
46.118.155.216	Ukraine	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.64.58	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/6/109176.pdf	Block	1

02-26-2016-05:04:08 to 02-26-2016-06:04:08