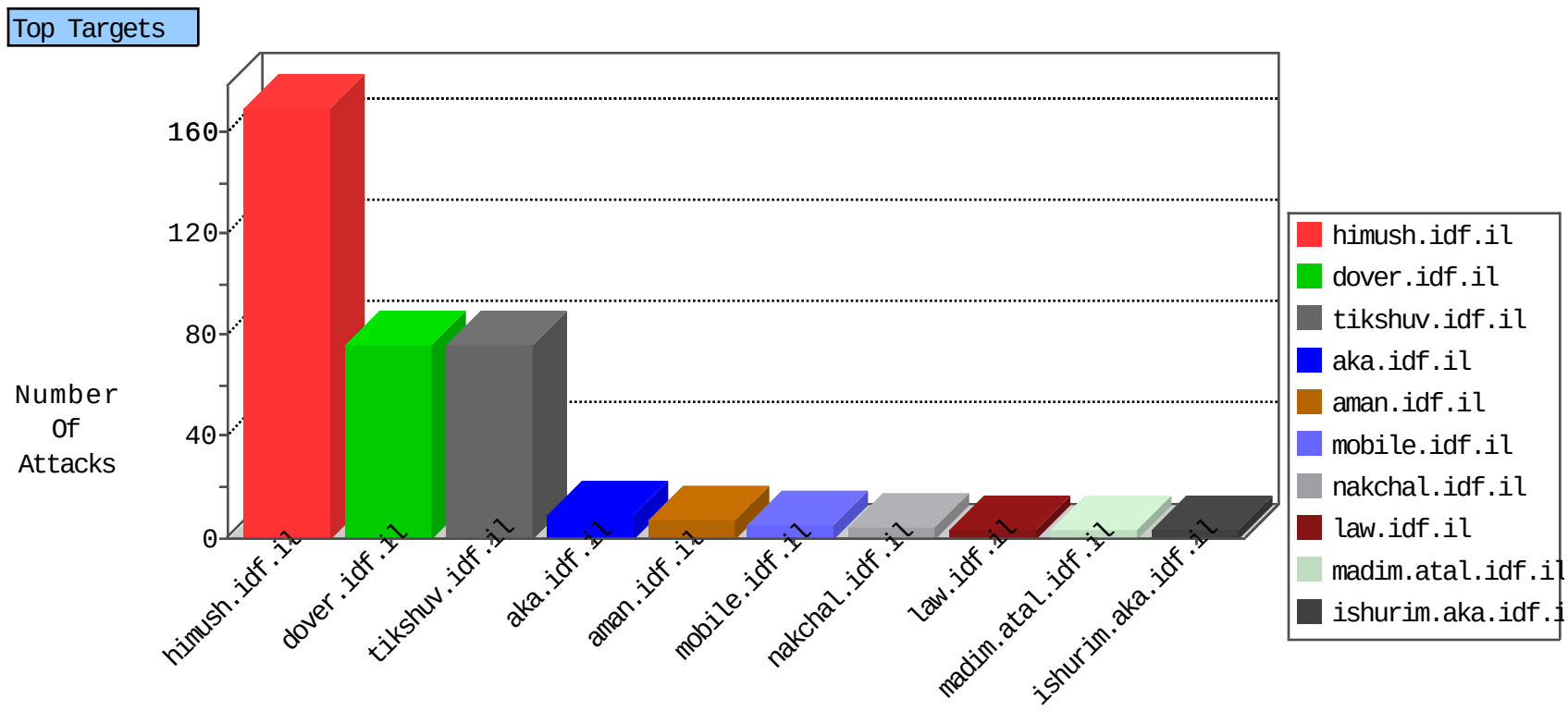
02-03-2016-03:04:05 to 02-03-2016-04:04:05

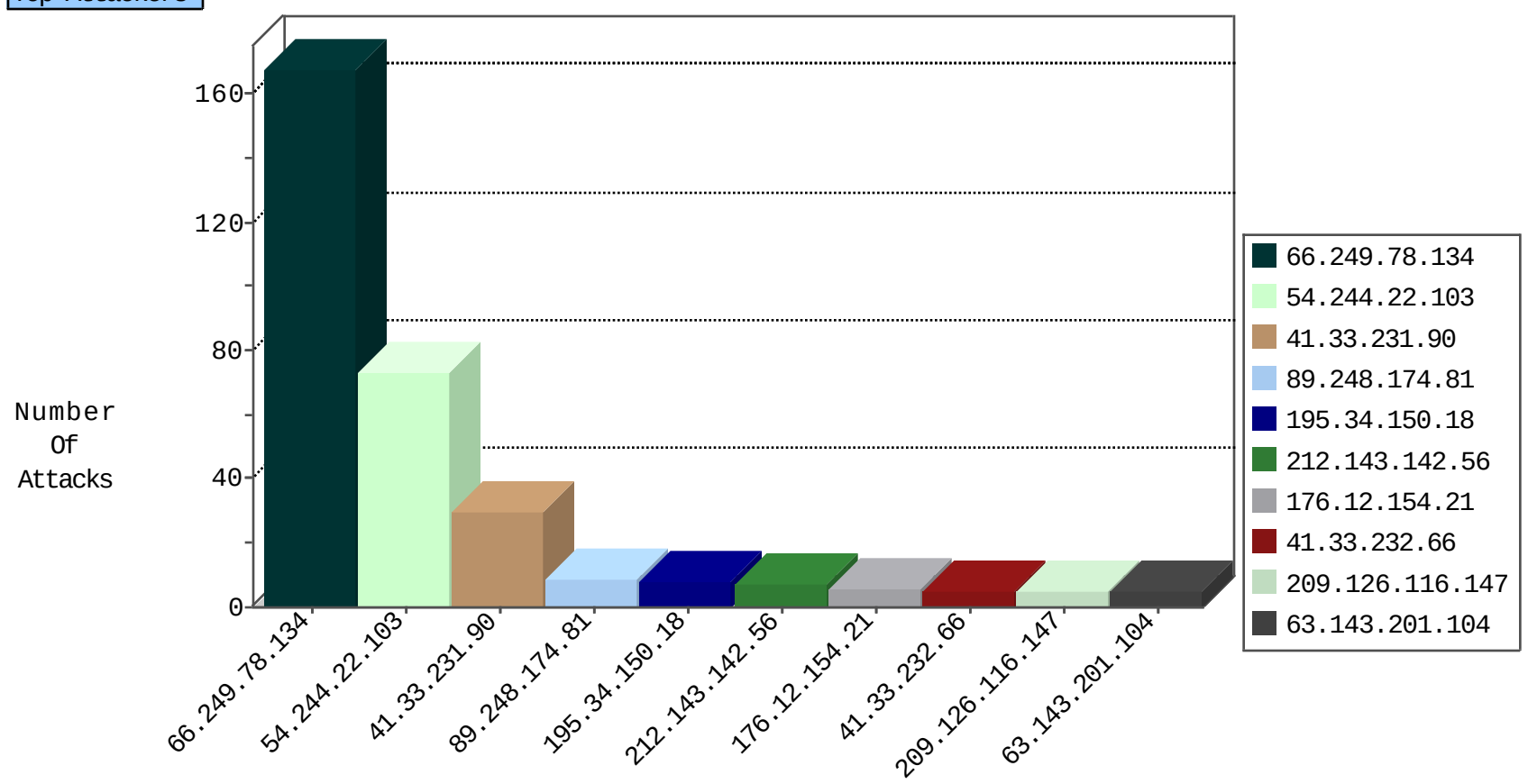
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

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

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	drop	4
192.118.64.213	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
185.35.62.239	Switzerland	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
142.54.160.210	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	drop	1
185.35.62.149	Switzerland	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

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

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.97.116.136	Ukraine	147.237.77.233	atal.idf.il	C108: HTTP: Trying to locate existing FCKeditor	Block	2
188.165.15.132	France	147.237.77.216	dover.idf.il	C228: HTTP: AhrefBot crawler	Block	1

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

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.78.134	147.237.76.30	United States	himush.idf.il	ET SCAN NMAP -sA (2)	168
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.78.216	147.237.77.243	United States	mobile.idf.il	ET SCAN NMAP -sA (2)	2
89.248.174.81	147.237.8.46	Netherlands	e.chinuch.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
210.93.50.130	147.237.72.156	Korea, Republic of	aman.idf.il	ET SCAN NMAP -f -sS	1
88.249.106.23	147.237.8.28	Turkey	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
145.255.2.133	147.237.0.17	Russian Federation	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
89.248.174.81	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.248.174.81	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.1.31.135	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
89.248.174.81	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.1.31.135	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
89.248.174.81	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
210.93.50.130	147.237.72.156	Korea, Republic of	aman.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.174.81	147.237.8.28	Netherlands	e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
209.126.116.147	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
145.255.2.133	147.237.0.34	Russian Federation	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
111.91.63.222	147.237.76.30	India	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
89.248.174.81	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.246.0.97	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 1024	1
89.248.174.81	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
218.1.31.135	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
89.248.174.81	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
210.93.50.130	147.237.72.156	Korea, Republic of	aman.idf.il	ET SCAN NMAP -sS window 2048	1

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

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	72
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
63.143.201.104	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
31.210.187.157	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.12.154.21	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
129.64.150.139	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
75.149.194.90	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
40.77.167.35	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
84.228.108.212	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
185.100.85.191		147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
98.140.61.66	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
61.135.190.71	China	147.237.0.35	akaws.idf.il	drop		drop	1
198.1.101.123	United States	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
141.212.122.198	United States	147.237.76.199	e.nakchal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1
84.228.108.212	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
216.218.206.106	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
188.120.148.197	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
123.125.71.32	China	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	1
61.135.190.197	China	147.237.0.33	idf.il	drop		drop	1
24.228.64.79	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.109.97.62	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.199	United States	147.237.76.199	e.nakchal.idf.i	Geo-location enforcement	Geo-location inbound enforcement	drop	1
84.228.108.212	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
50.150.50.153	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
123.125.71.32	China	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
209.126.116.147	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
86.44.122.147	Ireland	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
209.126.116.147	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
185.36.100.145	Anonymous Proxy	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
91.207.60.66	Ukraine	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
54.244.22.103	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	1
198.1.101.123	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1

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

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.154.21	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
188.143.232.11	Russian Federation	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 188.143.232.11	Block	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	1
188.143.232.11	Russian Federation	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/1111-he/	Block	1
37.147.33.61	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation &l in www.idf.il/templates/sendtofriend/sendtofriend.aspx	Block	1
104.131.245.20	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 104.131.245.20	Block	1
188.165.15.132	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
61.135.190.198	China	147.237.0.15	kosher-kravi.idf.i	Unauthorized URL Access to 147.237.0.15/	Block	1
209.2.234.242	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
66.249.64.190	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;docid in www.aka.idf.il/giyus/general/	None	1
185.100.85.191		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
66.249.78.146	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;catId in www.aka.idf.il/giyus/general/default.asp	None	1

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