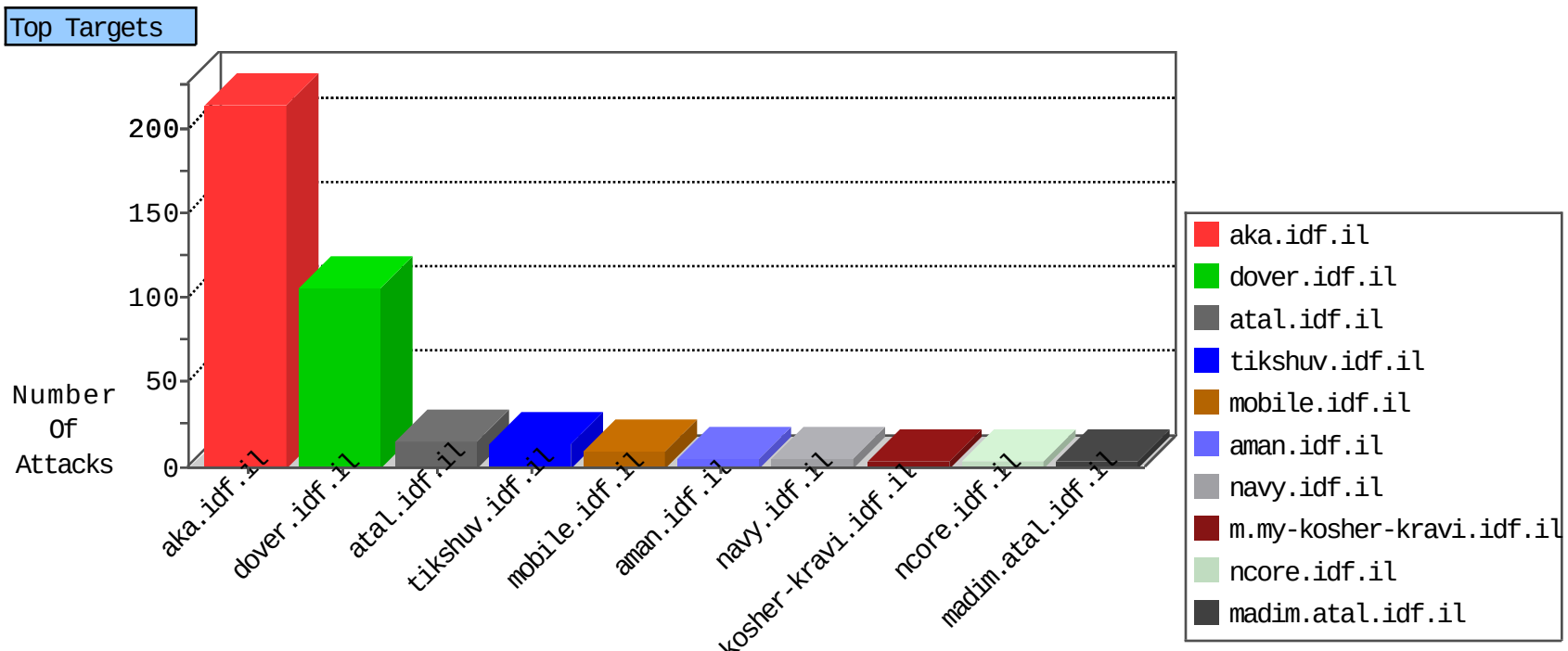
02-29-2016-04:04:03 to 02-29-2016-05:04:03

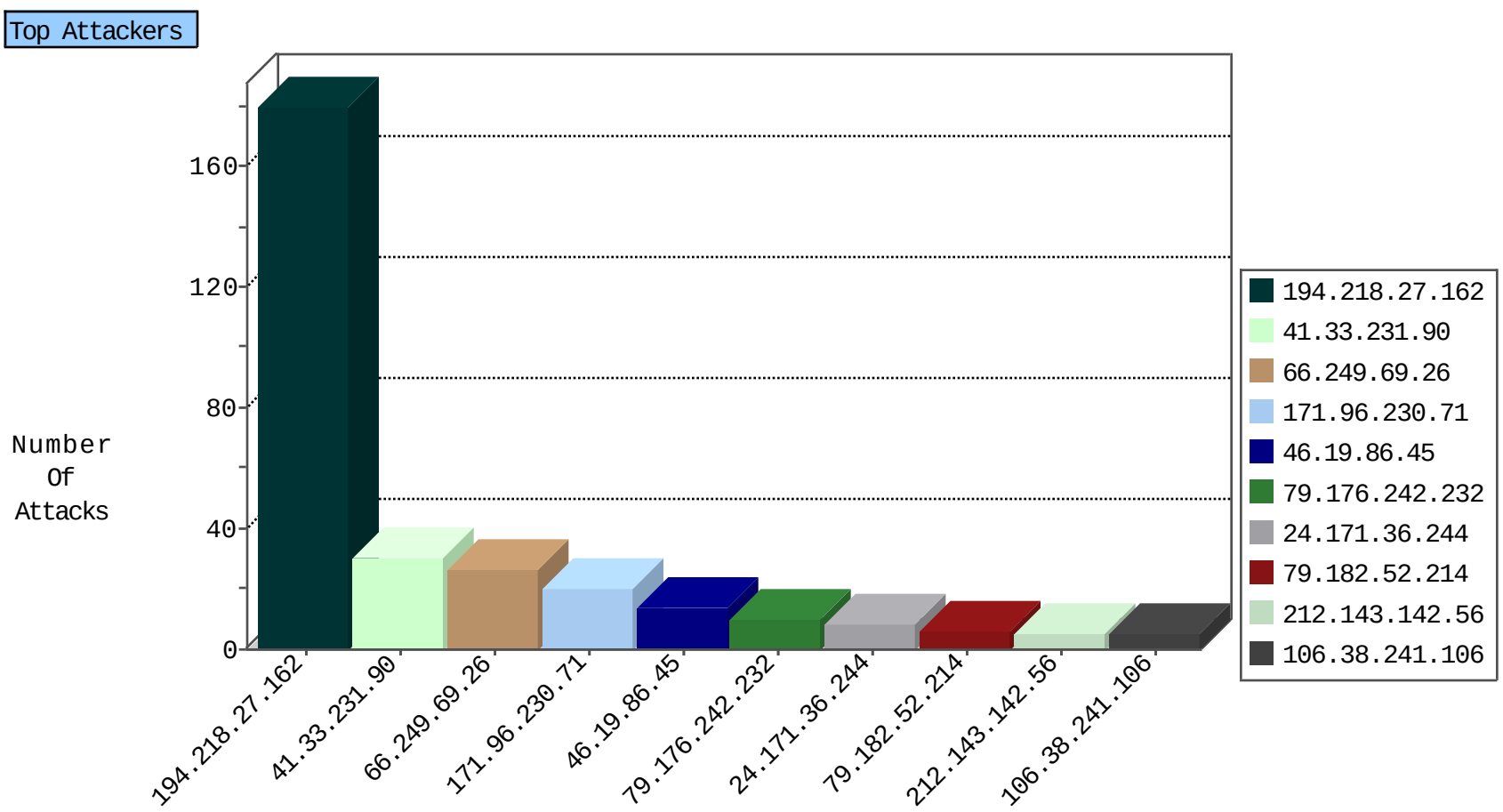
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-29-2016-04:04:03 to 02-29-2016-05:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
58.176.20.99	Hong Kong	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	4
198.84.107.122	United States	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
185.35.62.195	Switzerland	147.237.72.166	aka.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.201		147.237.77.19	law-forum.idf.il	Block_Udp_All_Nets	drop	1
115.230.124.164	China	147.237.0.33	idf.il	Invalid TCP Flags	drop	1
185.35.62.250	Switzerland	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1
66.240.219.146	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
198.84.107.122	United States	147.237.8.14	e.orchot.idf.il	Block_Ntp_All_Net	drop	1
124.44.70.1	Japan	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
24.171.36.244	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.56.28.67	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
71.6.135.131	United States	147.237.77.179	e.mazi.idf.il	Block_Udp_All_Nets	drop	1
198.84.107.122	United States	147.237.72.14	dover.idf.il(old)	Block_Ntp_All_Net	drop	1
141.212.122.208	United States	147.237.8.46	e.chinuch.idf.il	Block_Udp_All_Nets	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
185.56.28.67	Netherlands	147.237.77.235	sviva.idf.il	Block_Ntp_All_Net	drop	1
74.82.47.18	United States	147.237.0.33	idf.il	Block_Udp_All_Nets	drop	1

02-29-2016-04:04:03 to 02-29-2016-05:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.45	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
198.20.69.74	United States	147.237.8.27	e.madim.atal.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
66.249.64.180	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

02-29-2016-04:04:03 to 02-29-2016-05:04:03

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
202.71.25.29	147.237.76.177	India	ncore.idf.il	ET SCAN NMAP -sS window 2048	1
185.72.179.221	147.237.77.243		mobile.idf.il	ET SCAN Potential SSH Scan	1
138.36.0.3	147.237.77.176		matpash.idf.il	ET SCAN NMAP -sS window 1024	1
202.71.25.29	147.237.76.177	India	ncore.idf.il	ET SCAN NMAP -sS window 4096	1
202.71.25.29	147.237.76.177	India	ncore.idf.il	ET SCAN NMAP -f -sS	1
189.202.241.84	147.237.76.39	Mexico	mobile.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
185.72.179.221	147.237.77.205		prisha.idf.il	ET SCAN Potential SSH Scan	1

02-29-2016-04:04:03 to 02-29-2016-05:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	118
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	59
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
171.96.230.71	Thailand	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
79.176.242.232	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
24.171.36.244	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.182.52.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.45	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.86.45	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
130.193.37.19	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.24.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
93.158.152.6	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.0.146	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.145.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.140.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.170.226	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.131.124	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
79.178.195.113	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
5.22.131.124	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.67	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.38.241.106	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
74.82.47.34	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.174	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.162.108.191	France	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.161	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.45	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.171	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.68	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
106.38.241.106	China	147.237.77.233	atal.idf.il	drop	SAM rule	drop	1
221.199.217.173	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.174	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.162.108.191	France	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.165	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
138.36.0.3		147.237.76.202	e.halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.45	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.172	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
24.159.102.161	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.72	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
109.186.59.215	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.166	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
138.36.0.3		147.237.77.121	e.navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
198.20.69.74	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
71.28.45.27	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.173	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
24.159.102.161	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.73	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.116	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.167	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

02-29-2016-04:04:03 to 02-29-2016-05:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.69.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	24
66.249.66.15	United States	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.66.15	Block	3
66.249.66.18	United States	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.66.18	Block	3
66.249.66.18	United States	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 66.249.66.18	Block	2
66.249.78.87	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	2
66.249.66.21	United States	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.66.21	Block	2
66.249.69.26	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
74.82.47.2	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
157.55.39.105	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.176.242.232	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
66.249.78.80	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
37.142.159.100	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/newsarchive.aspx	Block	1
81.223.254.34	Austria	147.237.77.74	law.idf.il	Unauthorized URL Access to /robots.txt	Block	1
207.46.13.137	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/chamatz/miktzoa/default.asp	None	1
66.249.64.119	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 66.249.64.119	Block	1
99.237.178.220	Canada	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.78.94	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	1
66.249.64.119	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/yohalan/main/main.asp	Block	1
141.212.122.64	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to /x	Block	1

02-29-2016-04:04:03 to 02-29-2016-05:04:03