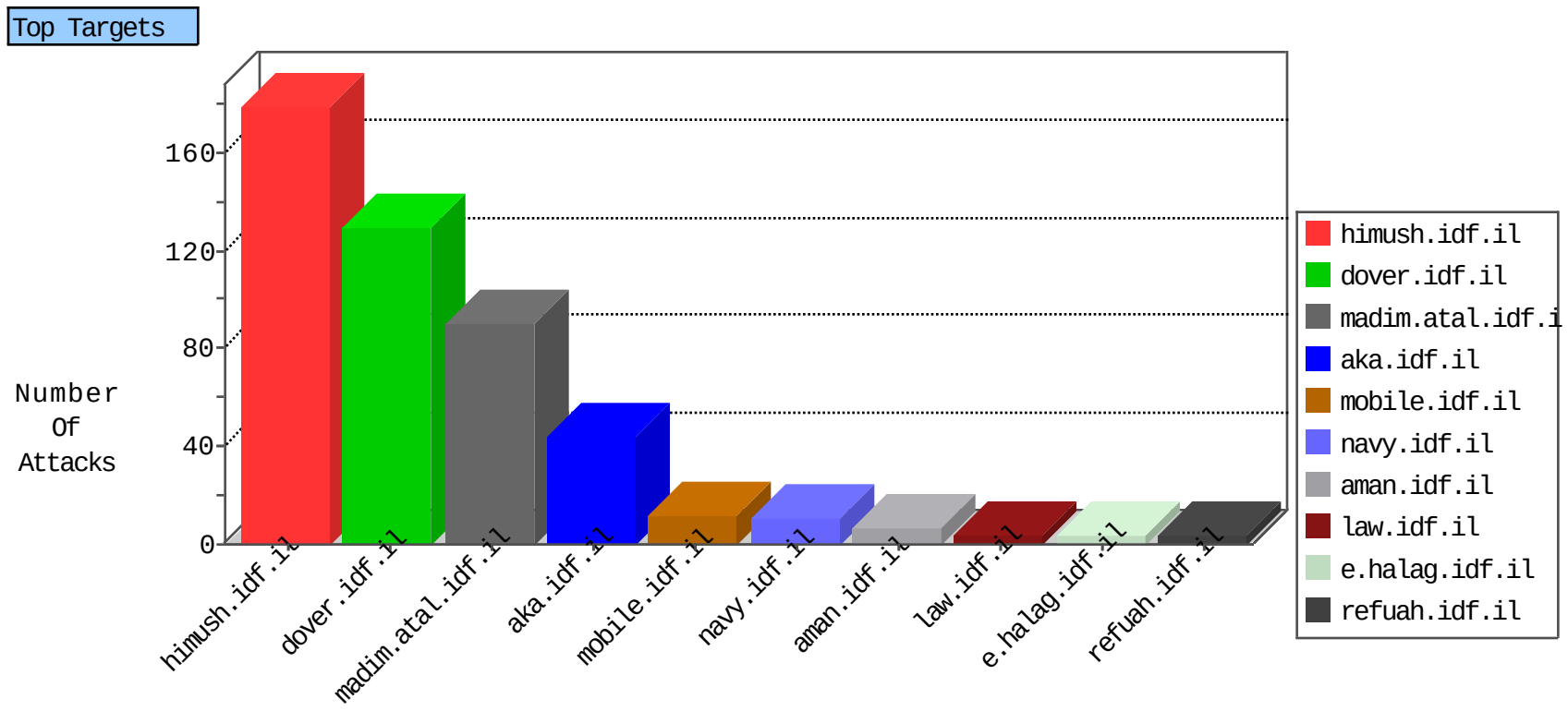
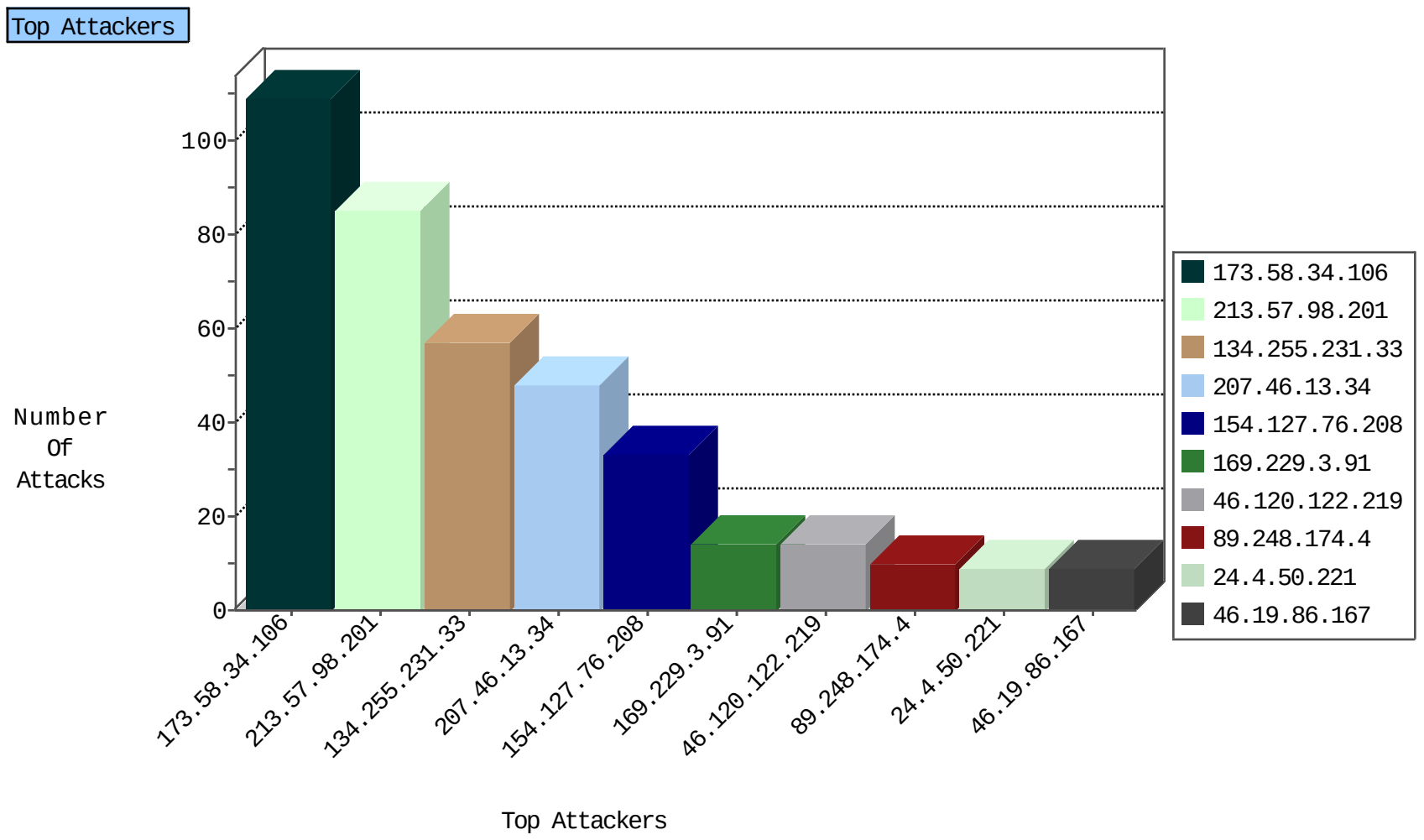
10-03-2016-01:06:05 to 10-03-2016-02:06:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



10-03-2016-01:06:05 to 10-03-2016-02:06:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.94.111.1	Russian Federation	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
58.218.200.137	China	147.237.76.177	ncore.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
71.6.167.142	United States	147.237.76.200	eitan.aka.idf.il	Black List	drop	1

10-03-2016-01:06:05 to 10-03-2016-02:06:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.254.9.215	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	3886: HTTP: Cross Site Scripting in POST Request	Block	4
92.238.226.245	United Kingdom	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
46.4.123.172	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
46.4.123.172	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

10-03-2016-01:06:05 to 10-03-2016-02:06:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
46.120.122.219	147.237.77.216	Israel	dover.idf.il	Xenu Link Sleuth User Agent	13
91.121.116.113	147.237.77.216	France	dover.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
151.80.41.177	147.237.72.166	France	aka.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
78.129.171.173	147.237.76.30	United Kingdom	himush.idf.il	ET SCAN Potential SSH Scan	1
77.126.34.193	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
58.218.200.137	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
50.84.213.146	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 4096	1
180.213.5.205	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
176.20.227.98	147.237.77.227	Denmark	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
14.152.59.11	147.237.72.167	China	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
121.223.248.67	147.237.8.50	Australia	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
78.140.61.49	147.237.76.42	Russian Federation	refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
78.129.171.173	147.237.8.50	United Kingdom	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
66.249.64.107	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
58.218.200.137	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
180.213.5.205	147.237.77.178	China	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
50.84.213.146	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 3072	1
180.213.5.205	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
46.120.122.219	147.237.77.74	Israel	law.idf.il	Xenu Link Sleuth User Agent	1

10-03-2016-01:06:05 to 10-03-2016-02:06:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
173.58.34.106	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	109
207.46.13.34	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	48
134.255.231.33	Germany	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
154.127.76.208	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
134.255.231.33	Germany	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	12
134.255.231.33	Germany	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	12
134.255.231.33	Germany	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
46.19.86.167	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
134.255.231.33	Germany	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
154.127.76.208	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	8
52.3.127.144	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	5
154.127.76.208	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
154.127.76.208	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
154.127.76.208	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
93.173.123.174	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	3
24.4.50.221	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
87.69.111.164	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
77.138.185.174	France	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.53.155.155	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.138.185.174	France	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
77.138.113.215	France	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
93.173.123.174	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
141.226.162.96	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
24.4.50.221	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
197.34.20.236	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
77.138.185.174	France	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
105.108.3.5	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
24.4.50.221	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	2
197.34.20.236	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
109.64.53.130	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
24.4.50.221	United States	147.237.76.30	himush.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	2
5.102.195.166	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	1
89.248.174.4	Netherlands	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.111	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
197.34.20.236	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.25	United States	147.237.76.148	gqcenter.aka.idf.i	drop		drop	1
181.67.143.160	Peru	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
52.3.127.144	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
109.253.130.80	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
169.229.3.91	United States	147.237.76.177	ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
37.26.147.138	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
89.248.174.4	Netherlands	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
2.55.156.204	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
89.248.174.4	Netherlands	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.104	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
195.62.53.168	Russian Federation	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
169.229.3.91	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
169.229.3.91	United States	147.237.0.35	akaws.idf.il	drop		drop	1
89.248.174.4	Netherlands	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

10-03-2016-01:06:05 to 10-03-2016-02:06:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.57.98.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	85
176.13.225.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
79.181.109.253	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.65.52	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
77.138.113.215	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
89.245.89.236	Germany	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.65.53	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
77.138.241.83	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/favicon.ico	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Untraceable SSL Sessions from 169.229.3.91 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
66.249.65.58	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8804-he/refuah.aspx	Block	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
66.249.76.58	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/news/<a href=	Block	1
82.81.30.52	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
46.120.56.126	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
207.46.13.73	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/documents.asp	Block	1
84.109.3.215	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1

10-03-2016-01:06:05 to 10-03-2016-02:06:05