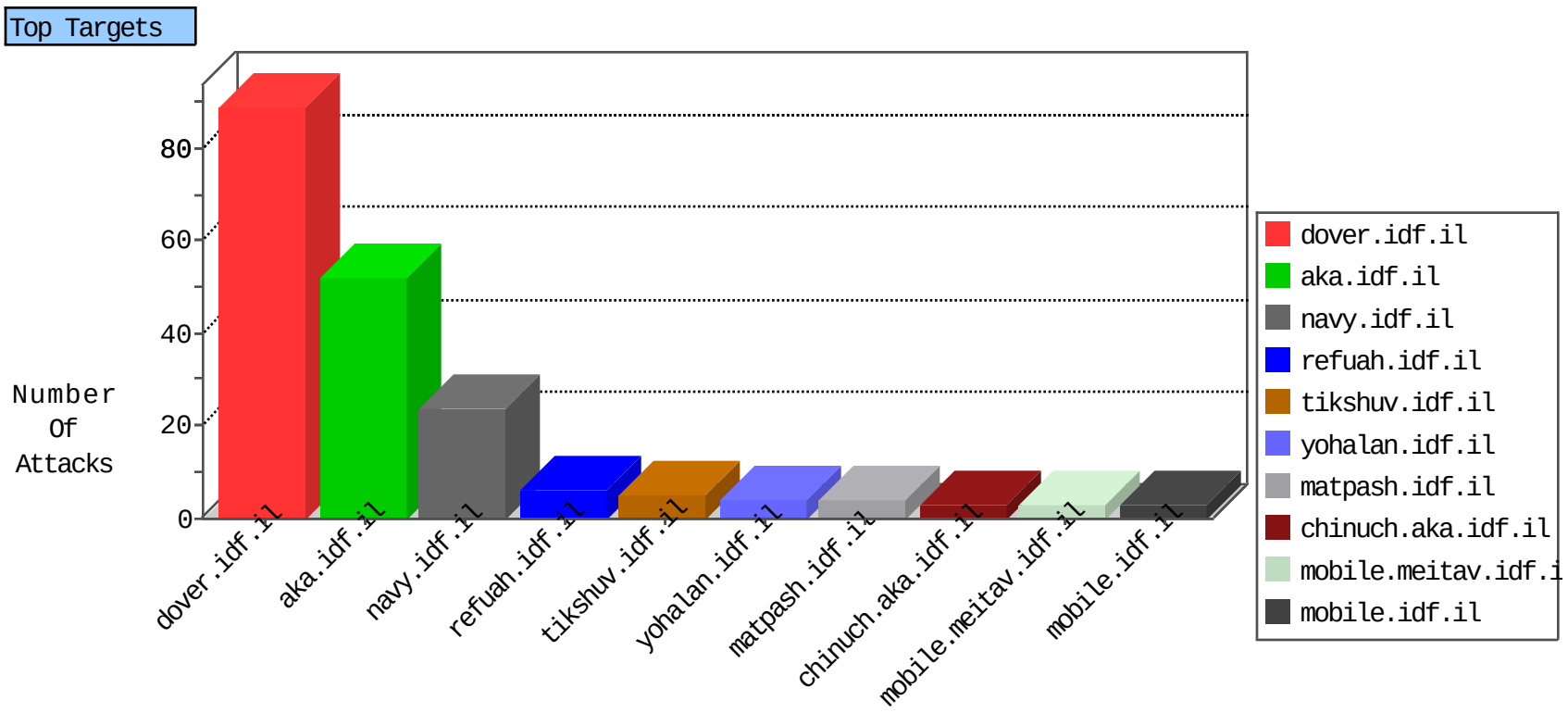
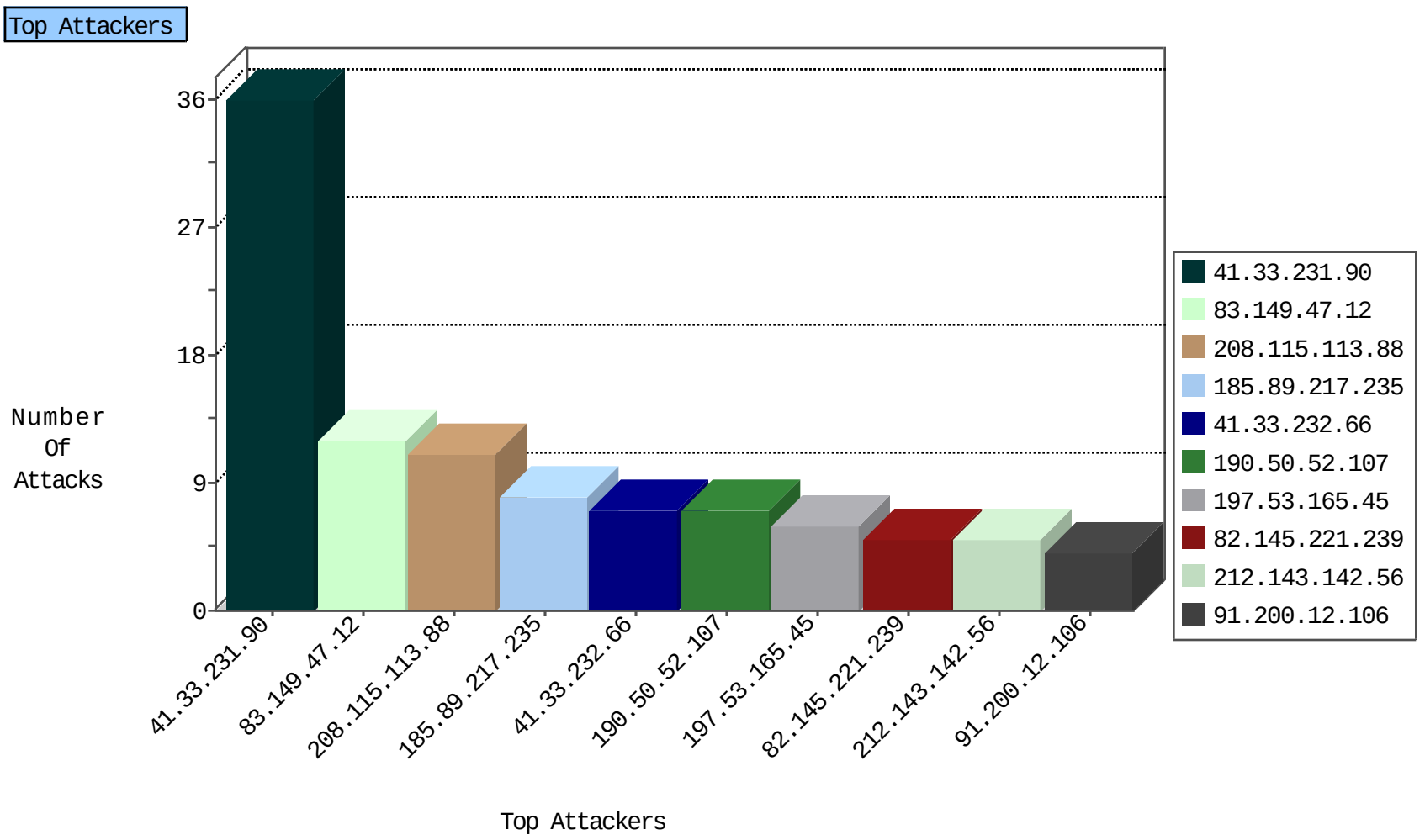
02-12-2016-04:04:08 to 02-12-2016-05:04:08

IDF Under Attack Daily Report





02-12-2016-04:04:08 to 02-12-2016-05:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.215	Israel	147.237.0.15	kosher-kravi.idf.il	TCP handshake violation, first packet not syn	drop	1181
222.186.34.37	China	147.237.76.86	navy.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
185.130.5.246		147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
158.130.6.191	United States	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
42.117.64.73	Vietnam	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.246		147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1
42.117.64.73	Vietnam	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.246		147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1

02-12-2016-04:04:08 to 02-12-2016-05:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-12-2016-04:04:08 to 02-12-2016-05:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	**Signature**	**Count**

02-12-2016-04:04:08 to 02-12-2016-05:04:08

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	34
185.89.217.235		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
190.50.52.107	Argentina	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
82.145.221.239	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
185.89.217.230		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
27.55.27.104	Thailand	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
86.104.167.220	Romania	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
66.249.65.14	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.173.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	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
130.193.51.66	Russian Federation	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.227.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.203.136.75	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	3
185.89.217.227		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
46.19.85.121	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
185.89.217.228		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
68.180.229.239	United States	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
136.243.67.234	Germany	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
104.219.200.105		147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
219.149.55.42	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
185.89.217.231		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
185.89.217.226		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
185.89.217.234		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
54.172.46.44	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
134.170.12.188	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
207.46.13.31	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.146	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.64	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
123.125.71.79	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
180.115.126.218	China	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
37.187.77.104	France	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
141.212.122.79	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
134.170.12.188	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
46.19.86.113	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.147	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
141.212.122.78	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
180.115.126.218	China	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
141.212.122.128	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
218.22.211.69	China	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
46.19.86.113	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.148	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
23.123.124.165	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.78	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
190.50.52.107	Argentina	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.12	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.96	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

02-12-2016-04:04:08 to 02-12-2016-05:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	10
83.149.47.12	Russian Federation	147.237.72.166	aka.idf.il	PHP Attempt	Block	6
83.149.47.12	Russian Federation	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 83.149.47.12	Block	5
2.54.145.1	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	2
217.132.125.79	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$71 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
195.154.226.90	France	147.237.77.216	dover.idf.il	Illegal HTTP Version HTTP/	Block	1
66.249.66.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/3338.jpg	Block	1
197.53.165.45	Egypt	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
197.53.165.45	Egypt	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
66.249.66.191	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/2389.jpg	Block	1
197.53.165.45	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
83.149.47.12	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/index.php	Block	1
8.37.71.79	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1038-he/dover.aspx&usg=alkjrhiqkvjz3dueqzptdrf61hjp-lgguw	Block	1
197.53.165.45	Egypt	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/xmlrpc.php	Block	1
72.167.232.200	United States	147.237.77.216	dover.idf.il	Directory Traversal (In URL)	Block	1
157.55.39.39	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
40.77.167.32	United States	147.237.72.166	aka.idf.il	Unknown Parameter 4f9c0c80 in www.aka.idf.il/main/home/default.aspx	None	1
197.53.165.45	Egypt	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
72.167.232.200	United States	147.237.77.216	dover.idf.il	Directory Traversal - 16	Block	1
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/main/home/pniot.aspx	Block	1
157.55.39.209	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_text.asp	Block	1
66.249.66.131	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/3493.jpg	Block	1
197.53.165.45	Egypt	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1

02-12-2016-04:04:08 to 02-12-2016-05:04:08