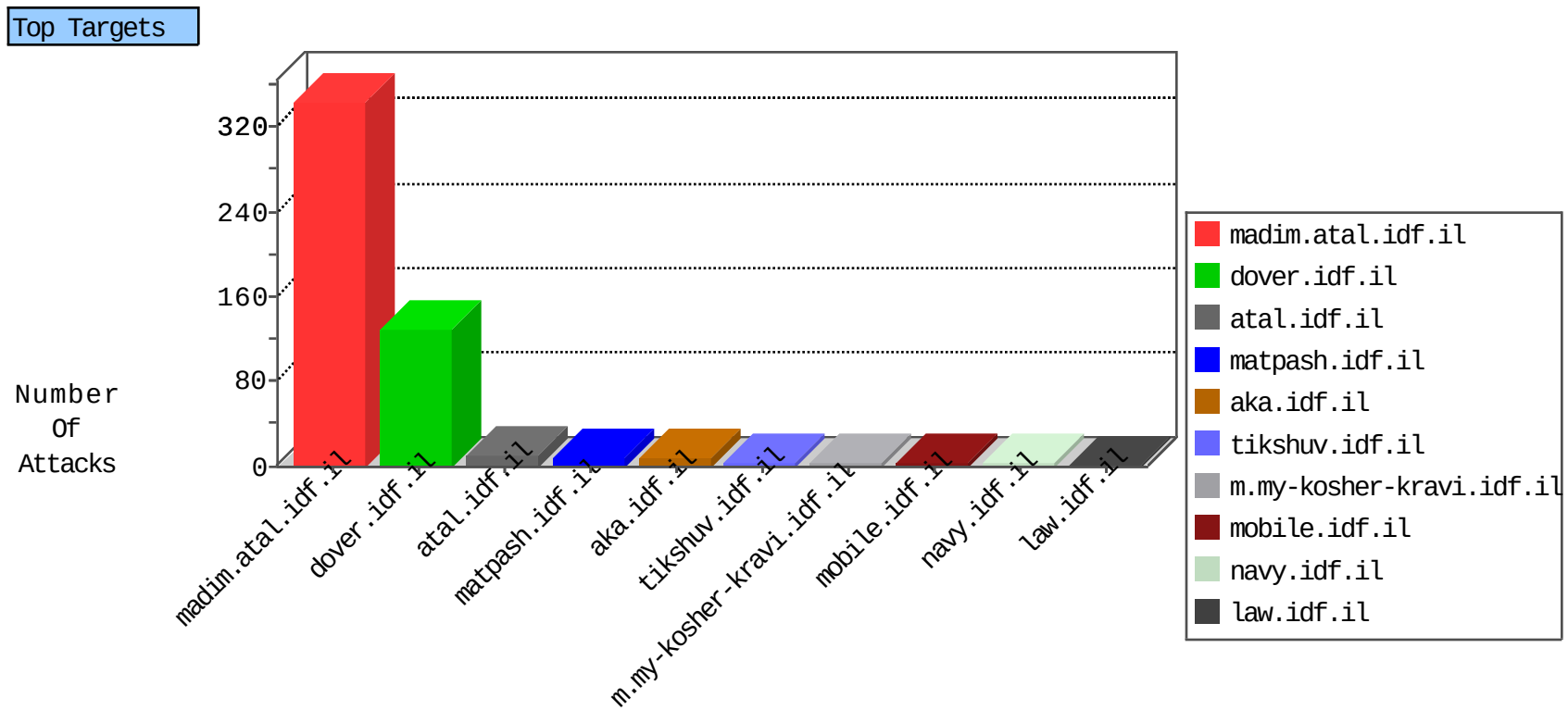
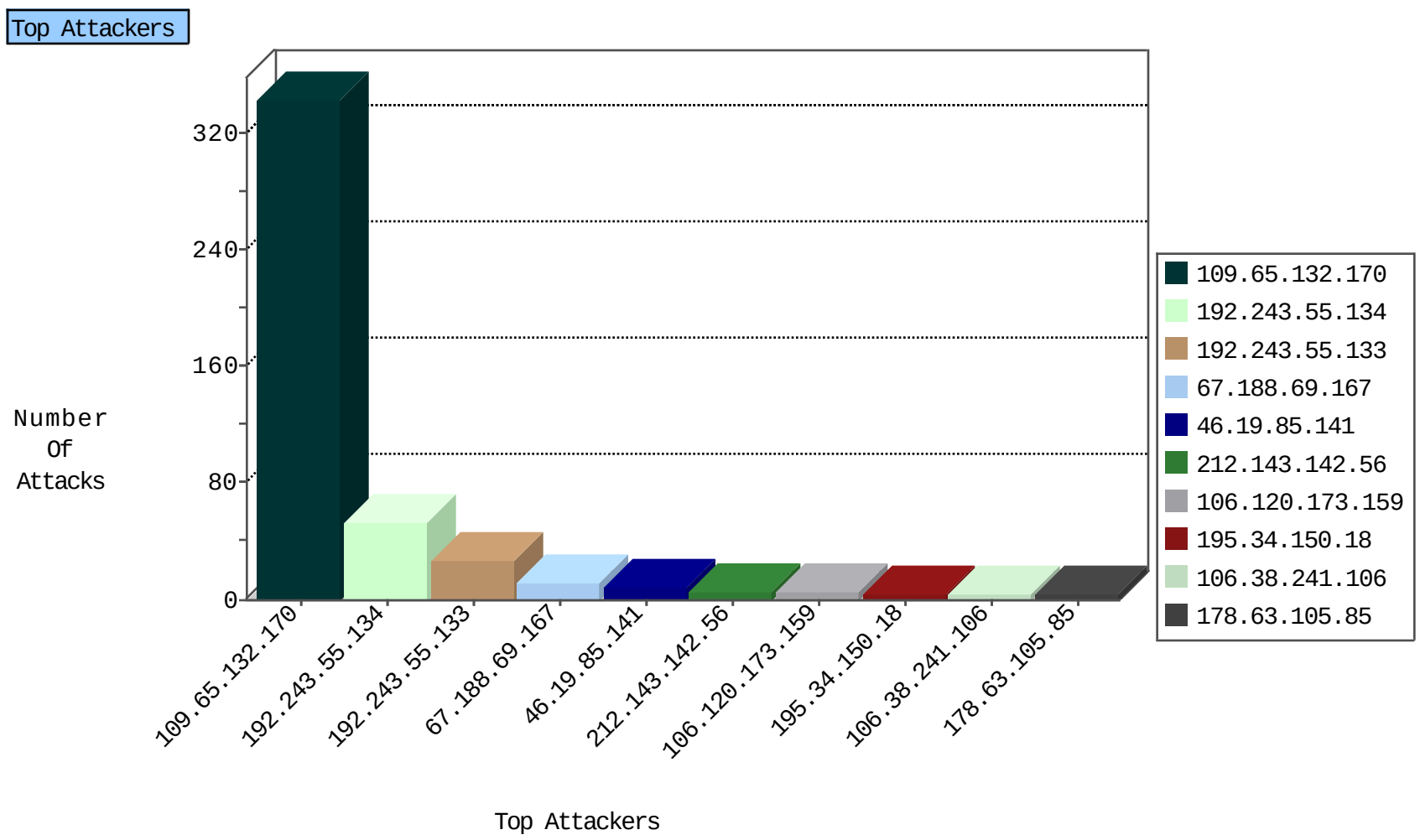
03-05-2016-05:04:09 to 03-05-2016-06:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-05-2016-05:04:09 to 03-05-2016-06:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
184.105.139.120	United States	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.76	United States	147.237.77.178	e.matpash.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.112	United States	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.68	United States	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
184.105.247.232	United States	147.237.77.61	e.cogat.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.88	United States	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
220.118.59.253	Korea, Republic of	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.112	United States	147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.68	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Ntp_All_Net	drop	1
198.20.87.98	United States	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.100	United States	147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1
74.82.47.6	United States	147.237.77.243	mobile.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.120	United States	147.237.8.46	e.chinuch.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.76	United States	147.237.72.166	aka.idf.il	Block_Ntp_All_Net	drop	1
200.43.219.114	Argentina	147.237.0.33	idf.il	JLM_Purple_Con_Limit_Http	drop	1
184.105.139.104	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1

03-05-2016-05:04:09 to 03-05-2016-06:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	6
197.41.75.76	Egypt	147.237.77.216	dover.idf.il	12026: HTTP: LOIC DDoS Tool (ONLY enable when under DoS attack)	Block	1
207.46.13.70	United States	147.237.0.34	tikshuv.idf.i	C1000138: HTTP: prefix 1.01 in the URL	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
151.80.31.113	Italy	147.237.0.34	tikshuv.idf.i	C1000146: HTTP: AhrefBot crawler	Block	1

03-05-2016-05:04:09 to 03-05-2016-06:04:09

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
223.79.6.99	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -f -sS	1
196.47.173.21	147.237.8.45	Cote D'Ivoire	e.eitan.idf.il	ET SCAN NMAP -sS window 3072	1
112.196.49.101	147.237.77.216	India	dover.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	147.237.77.179	Canada	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
196.47.173.21	147.237.8.45	Cote D'Ivoire	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
104.215.89.20	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 3072	1

03-05-2016-05:04:09 to 03-05-2016-06:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
67.188.69.167	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	10
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.141	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
106.38.241.106	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
5.22.131.14	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
178.63.105.85	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	1
103.41.177.26		147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
212.71.235.23	United Kingdom	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
8.37.227.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
184.105.139.111	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
139.162.152.84	Netherlands	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.34	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
178.63.105.85	Germany	147.237.72.167	ishurim.aka.idf.il	drop	SAM rule	drop	1
184.105.247.211	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
139.162.152.84	Netherlands	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.56	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
195.62.53.168	Russian Federation	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
178.63.105.85	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	1
216.218.206.78	United States	147.237.0.16	my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
64.19.78.243	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	1
146.185.239.102	Russian Federation	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
76.189.160.78	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
197.231.221.211	Liberia	147.237.0.35	akaws.idf.il	drop		drop	1
8.37.227.68	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
184.105.139.103	United States	147.237.76.39	mobile.meitav.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
216.218.206.119	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
64.19.78.243	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
178.63.105.85	Germany	147.237.0.17	m.my-kosher-kravi.idf.il	drop	SAM rule	drop	1
79.178.3.239	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
200.43.219.114	Argentina	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
8.37.227.69	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
184.105.139.107	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
130.193.51.51	Russian Federation	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1

03-05-2016-05:04:09 to 03-05-2016-06:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.65.132.170	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	344
195.154.173.103	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	3
149.88.71.234	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.249.65.18	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1877	Block	1
157.55.39.145	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/main/giyus/giyus/general.aspx	Block	1
37.26.148.129	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1362-he/dover.aspx	Block	1
185.106.94.30		147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/xmlrpc.php	Block	1
40.77.167.62	United States	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/	Block	1
185.112.248.32		147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to 147.237.76.147/	Block	1
64.19.78.243	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
149.88.71.234	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 149.88.71.234 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/movies/yassin7.	Block	1
66.249.65.18	United States	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.65.18	Block	1

03-05-2016-05:04:09 to 03-05-2016-06:04:09