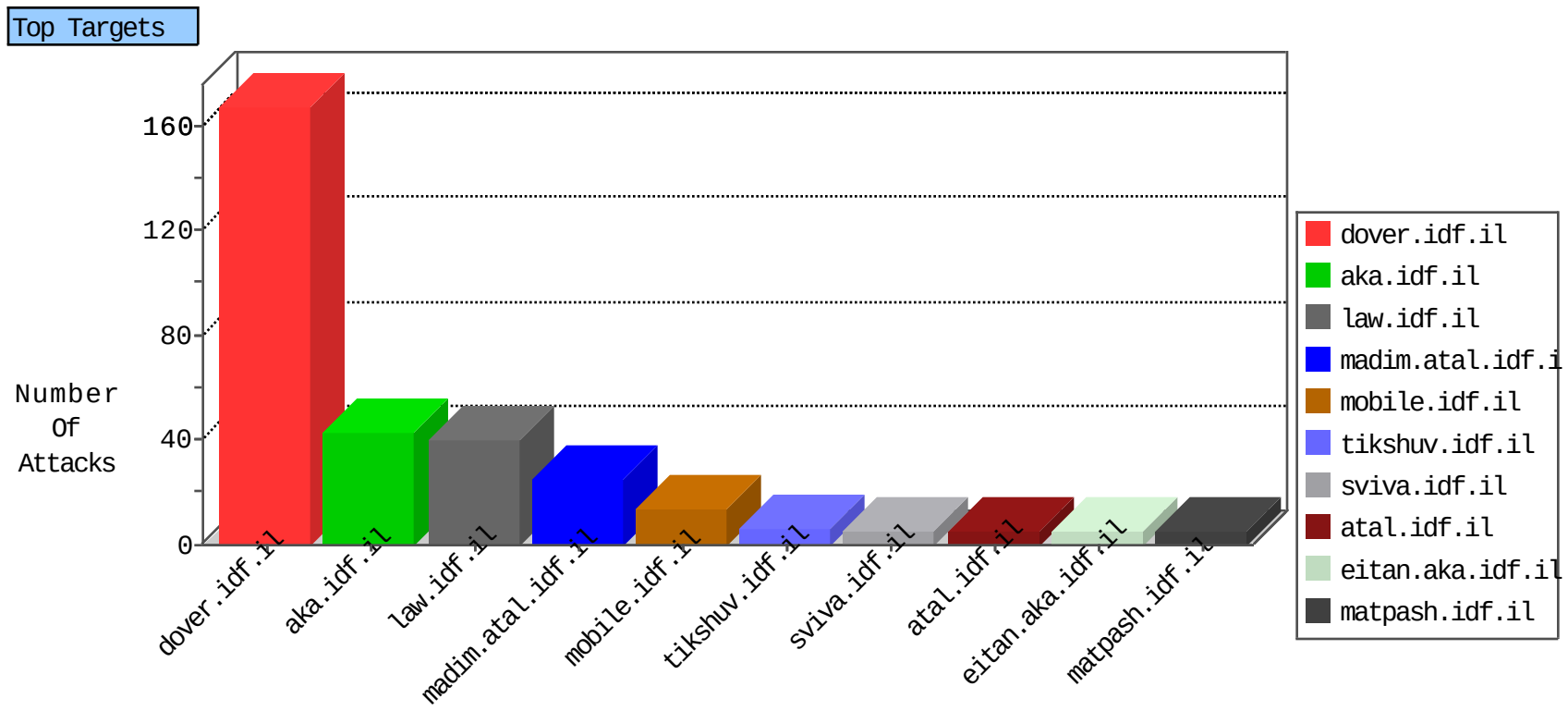
03-04-2016-06:04:06 to 03-04-2016-07:04:06

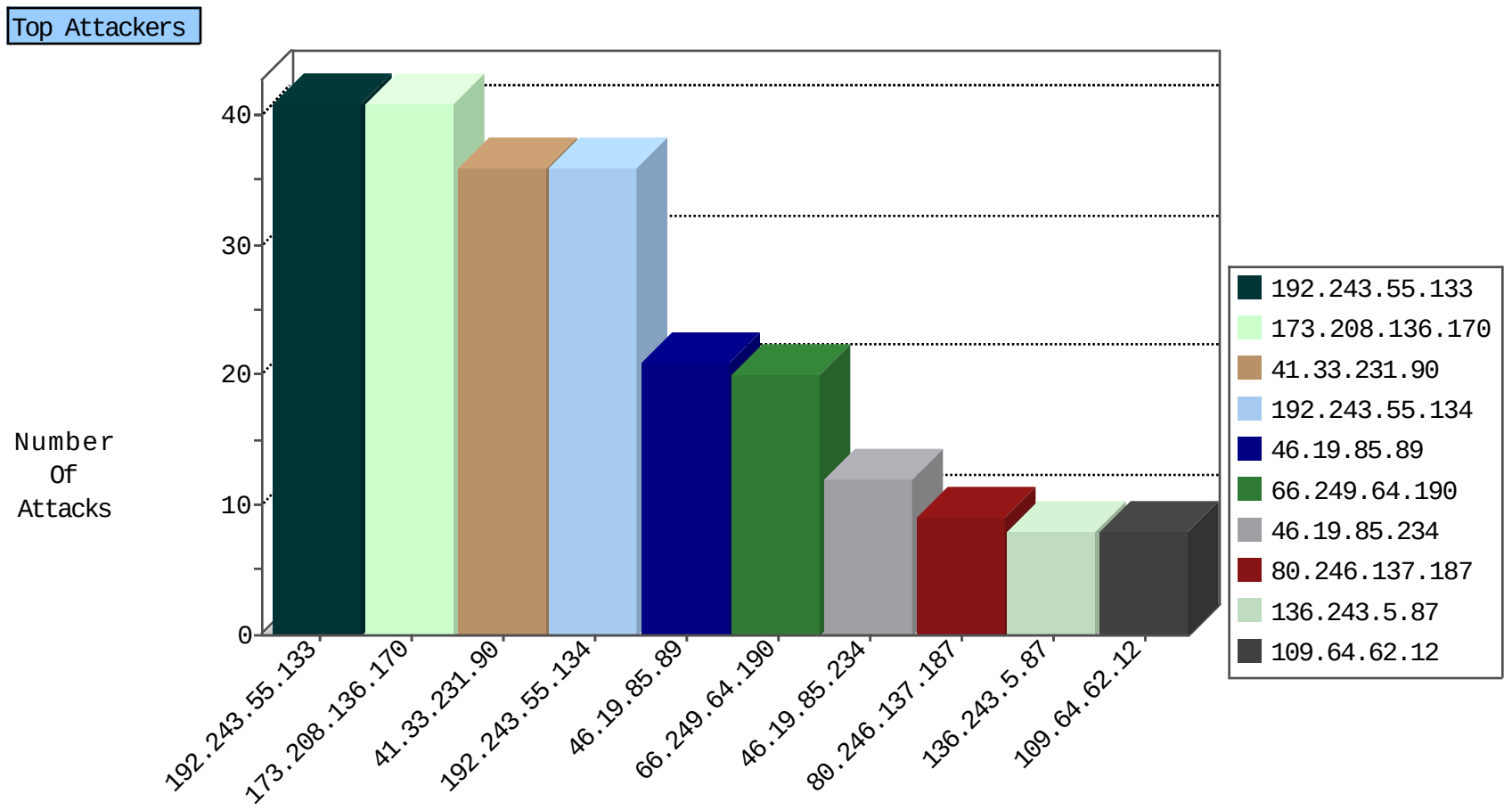
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

03-04-2016-06:04:06 to 03-04-2016-07:04:06

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
184.105.139.80	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1
213.238.176.44	Turkey	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
67.169.173.142	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
185.35.62.79	Switzerland	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	1
213.238.176.44	Turkey	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
69.64.57.170	United States	147.237.77.235	sviva.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.77.227	e.hamaz.idf.il	Block_Udp_All_Nets	drop	1
213.238.176.44	Turkey	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1

03-04-2016-06:04:06 to 03-04-2016-07:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.188.192	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
185.106.92.164		147.237.77.235	sviva.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	2
37.142.210.27	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
51.255.162.167	United Kingdom	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
193.111.140.106	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
85.14.244.113	Germany	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-04-2016-06:04:06 to 03-04-2016-07:04:06

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
42.203.50.219	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.0.34	China	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
122.141.236.69	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
122.141.236.69	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.193	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.113	147.237.77.227	Ukraine	e.hamaz.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
42.203.50.219	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
222.186.21.181	147.237.0.35	China	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
195.216.176.244	147.237.76.200	Latvia	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
177.23.168.183	147.237.76.31	Brazil	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
122.141.236.69	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
122.141.236.69	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.113	147.237.77.227	Ukraine	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.64.253	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1

03-04-2016-06:04:06 to 03-04-2016-07:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
173.208.136.170	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	41
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
136.243.5.87	Germany	147.237.77.216	dover.idf.il	drop	SAM rule	drop	6
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.65.235.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.137.187	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
65.55.210.110	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.134	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
122.201.19.22	Mongolia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.64.62.12	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
192.243.55.133	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
136.243.5.87	Germany	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
192.243.55.133	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	2
37.142.182.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	2
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
5.102.242.54	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	2
37.142.182.168	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
74.82.47.23	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.106.92.164		147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
95.38.61.199	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
50.138.246.215	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.90	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
121.54.32.147	Philippines	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.32	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.106.94.49		147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
95.38.61.199	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.112	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.218.206.115	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.44	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.234	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

03-04-2016-06:04:06 to 03-04-2016-07:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
109.64.62.12	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	5
66.249.64.190	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.190	Block	5
80.246.137.187	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
66.249.64.233	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/	Block	2
207.46.13.70	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1503-en/dover.aspx.	Block	1
66.249.64.253	United States	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
185.120.126.82		147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
66.249.75.143	United States	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/894-he	Block	1
66.249.66.67	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
185.120.126.82		147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 185.120.126.82	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1038-ar/cogat.aspx	Block	1
180.76.15.156	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/shared/clientscripts/{1}	Block	1
66.249.66.126	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/pdf/files/7/109397.pdf	Block	1
185.120.126.82		147.237.76.86	navy.idf.il	PHP Attempt	Block	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/shalishut/site/faq.aspx	None	1
185.99.32.3		147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.66.176	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/6/976.pdf	Block	1
188.138.1.218	Germany	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to 147.237.76.147/	Block	1
185.120.126.82		147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
66.249.75.143	United States	147.237.76.147	chinuch.aka.idf.i	Multiple Unauthorized URL Access from 66.249.75.143	Block	1

03-04-2016-06:04:06 to 03-04-2016-07:04:06