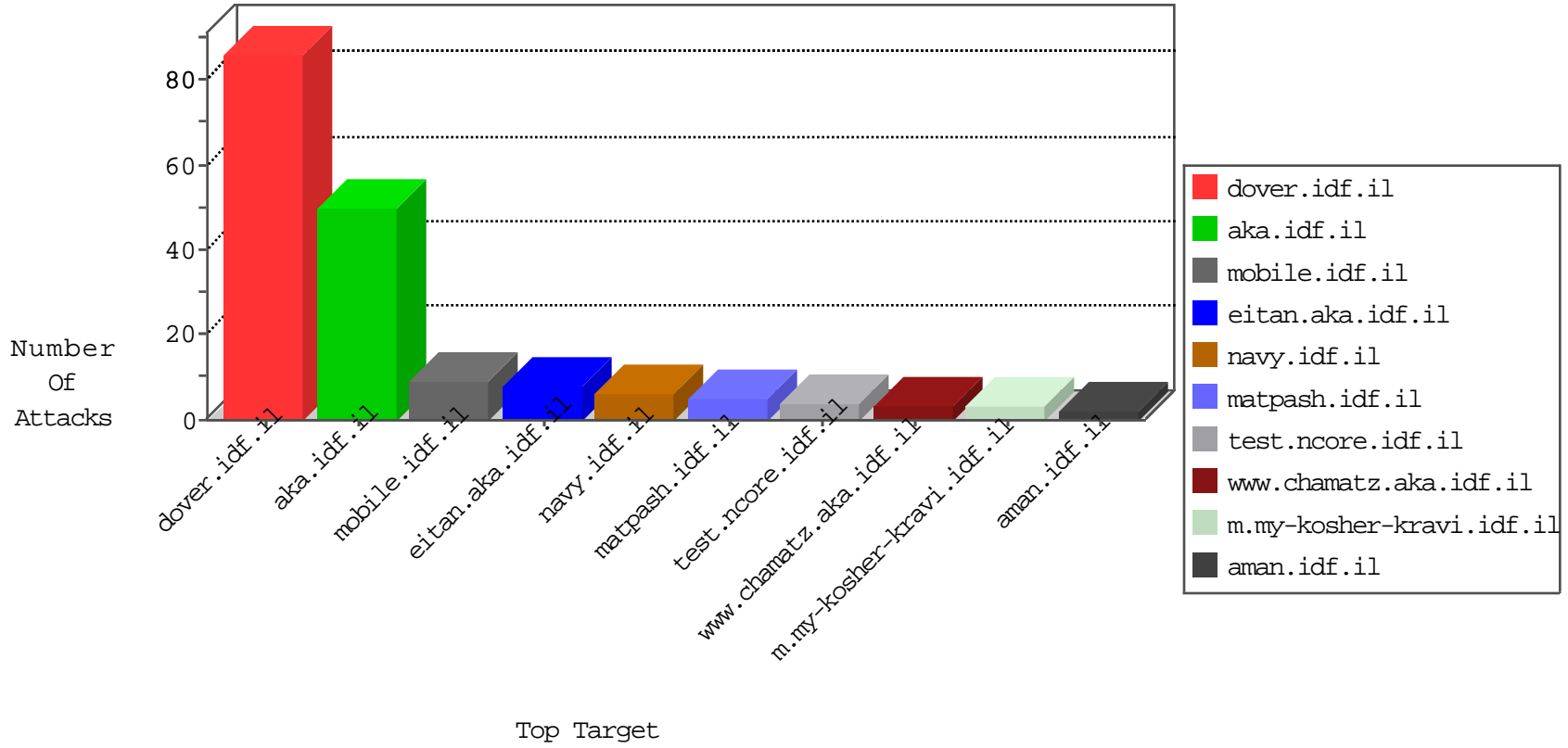


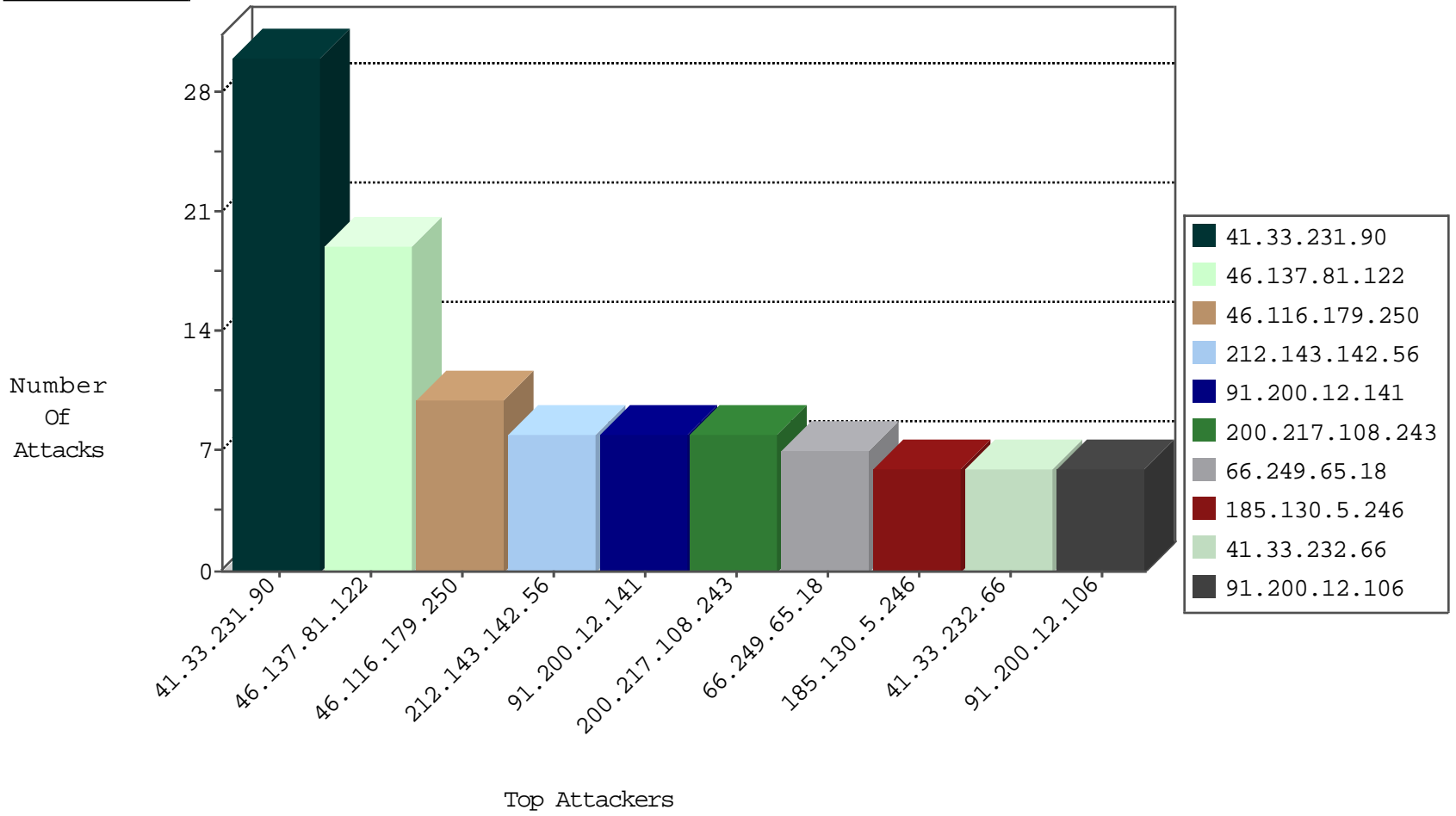
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.130.5.246		147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	1
142.54.160.211	United States	147.237.77.216	dover.idf.il	block-sp-trafl	drop	1
185.130.5.246		147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.246		147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.76.198	e.yohalan.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.246		147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.224		147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.246		147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
74.91.28.58	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-trafl	forward	1
185.130.5.246		147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.9.87.111	Germany	147.237.77.226	www.chamatz.aka.idf.il	C106: HTTP: majestic bot	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
------------------	----------------	------------------	------	-----------	-------

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	30
46.137.81.122	Ireland	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
46.116.179.250	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.65.18	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
200.217.108.243	Brazil	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
168.187.116.186	Kuwait	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
91.200.12.141	Ukraine	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
91.200.12.141	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
107.167.103.82	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
149.78.22.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.154.160.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.233.76.49	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
199.201.64.132	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.94.164.87	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
200.217.108.243	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
169.237.145.68	United States	147.237.76.86	navy.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
91.200.12.106	Ukraine	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
185.32.179.165	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.116.179.250	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
91.200.12.106	Ukraine	147.237.76.200	eitan.aka.idf.il	drop	SAM rule	drop	2
46.137.81.122	Ireland	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	2
2.54.63.102	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
81.169.237.146	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	2
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
141.212.122.138	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
130.203.136.75	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
184.32.210.61	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.143	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.73	United States	147.237.0.33	idf.il	drop		drop	1
37.187.131.217	France	147.237.72.14	dover.idf.il(old)	drop	SAM rule	drop	1
141.212.122.139	United States	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.64	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.3.144.120	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.148	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.74	United States	147.237.0.33	idf.il	drop		drop	1
81.169.237.146	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	1
37.187.131.217	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
141.212.122.141	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.65	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.149	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.133	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
81.169.237.146	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
176.13.22.76	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.142	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.68	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
146.185.239.102	Russian Federation	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
109.253.215.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
66.249.66.131	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/9/2969.jpg	Block	1
185.120.126.201		147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/default.asp	Block	1
46.137.81.122	Ireland	147.237.72.166	aka.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	None	1
213.8.204.32	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
84.108.136.252	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
66.249.66.191	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
185.120.126.201		147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 185.120.126.201	Block	1
74.91.28.58	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to www.1916wh.com/	Block	1
46.137.81.122	Ireland	147.237.72.166	aka.idf.il	Multiple signatures from 46.137.81.122	Block	1
100.6.0.249	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
66.249.78.80	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
185.120.126.201		147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	1
84.108.136.252	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
66.249.65.18	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
68.180.228.175	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
41.130.180.60	Egypt	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
194.187.168.215	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
84.108.136.252	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
185.120.126.201		147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
68.180.229.94	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
41.130.180.60	Egypt	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
207.46.13.58	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.58	Block	1
84.108.136.252	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1