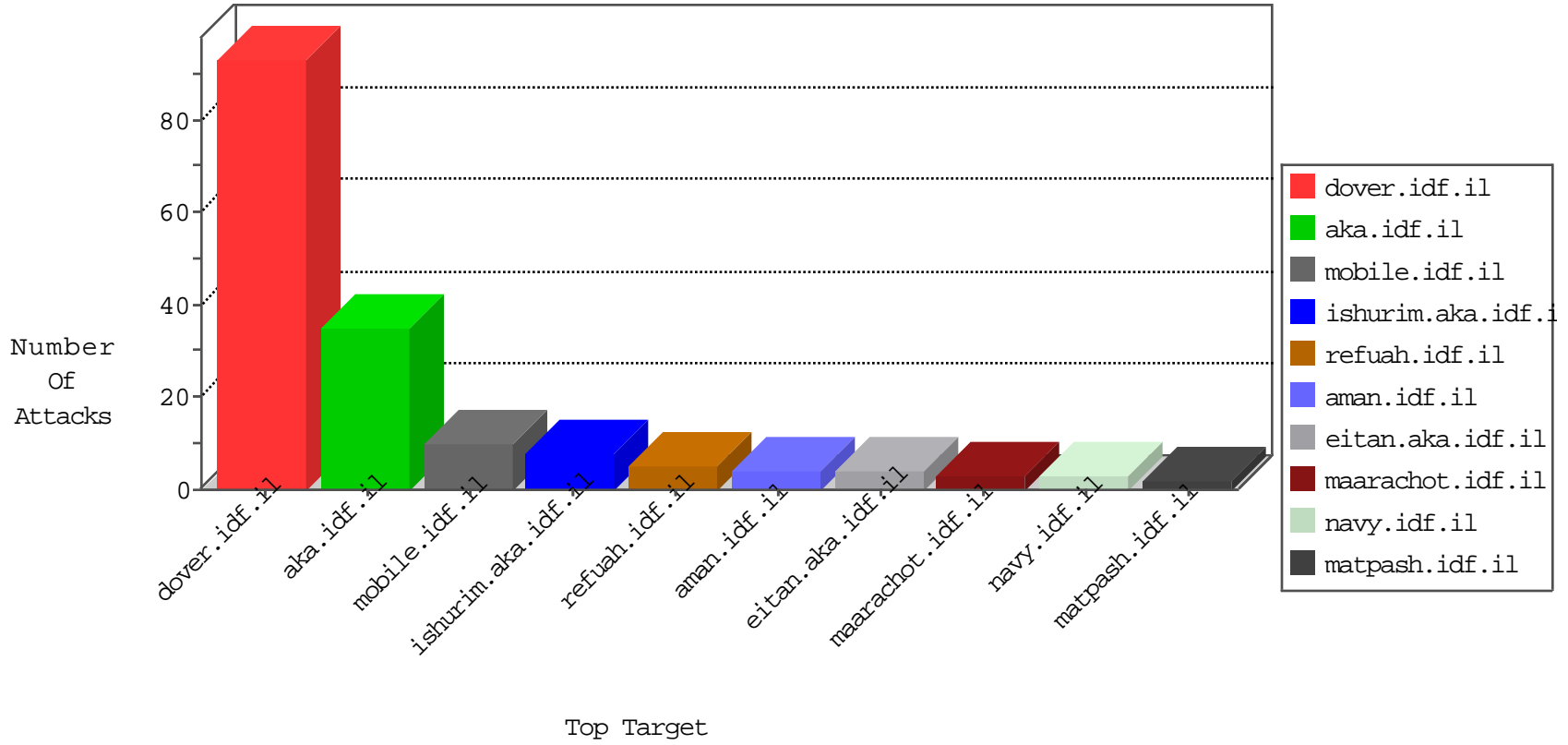


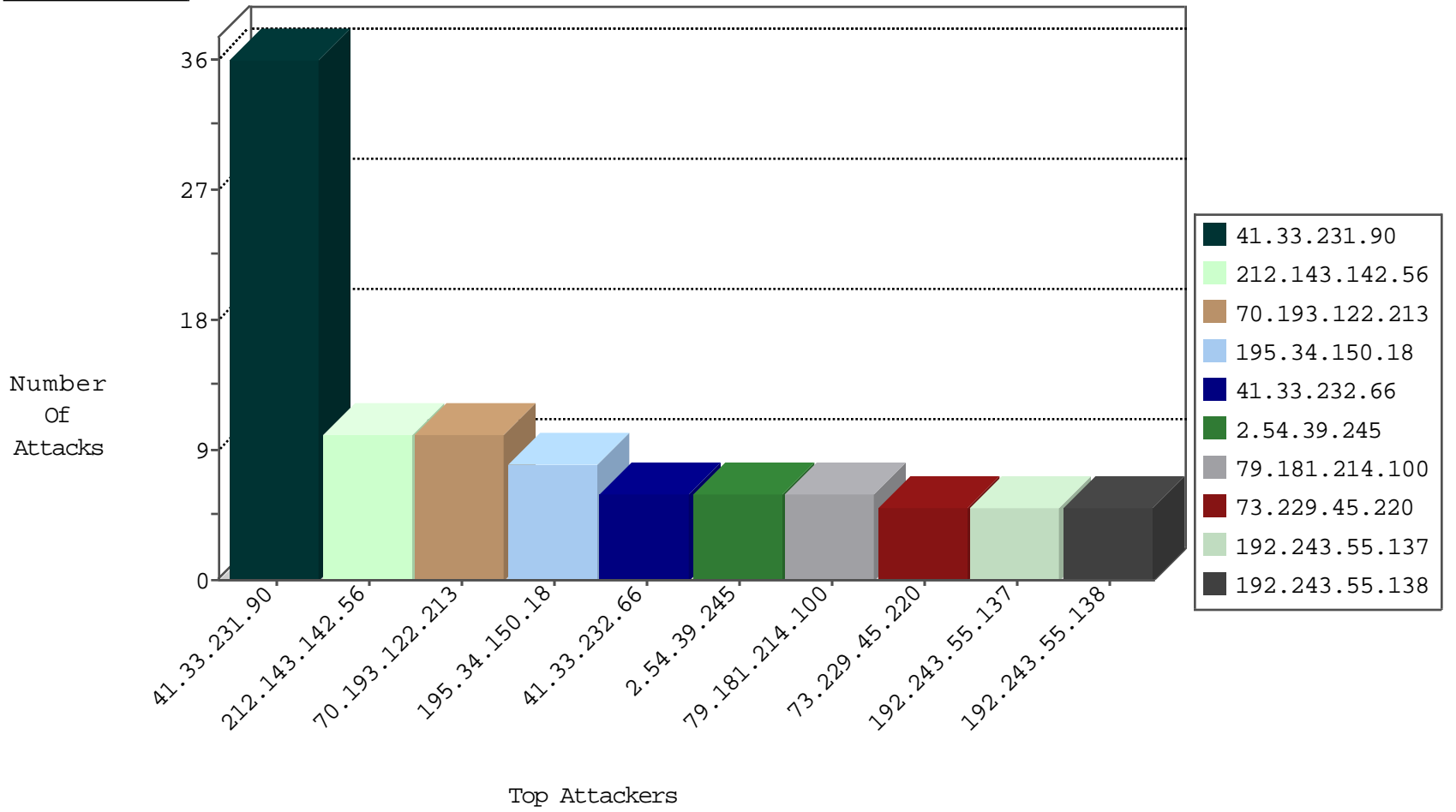
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.42.253.132	United States	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1
146.185.239.100	Russian Federation	147.237.72.167	ishurim.aka.idf.il	block-sp-trafl	drop	1

Top Attackers In IPS

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

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
115.231.9.148	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
94.102.51.38	147.237.72.166	Netherlands	aka.idf.il	ET SCAN NMAP -sS window 1024	1
36.72.228.72	147.237.72.156	Indonesia	aman.idf.il	ET SCAN NMAP -sS window 4096	1
218.246.0.97	147.237.77.243	China	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
114.112.90.54	147.237.0.19	China	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
45.79.10.124	147.237.76.200		eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
36.72.228.72	147.237.72.156	Indonesia	aman.idf.il	ET SCAN NMAP -sS window 1024	1
201.48.50.33	147.237.0.34	Brazil	tikshuv.idf.il	ET SCAN Potential SSH Scan	1

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	36
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
2.54.39.245	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.214.100	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
70.193.122.213	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
73.49.99.218	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
70.193.122.213	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
79.177.116.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
52.49.79.6	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
46.19.86.51	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.160.196.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
50.18.94.121	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
46.121.27.29	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
45.79.10.124		147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
31.210.186.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.121.27.29	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
37.187.114.171	France	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.219	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
198.1.101.123	United States	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
149.78.56.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
37.187.114.171	France	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.224	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
212.124.109.166	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
5.22.131.107	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
149.78.56.220	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
46.121.86.104	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
188.152.234.175	Italy	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
37.187.114.171	France	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
88.75.61.15	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
54.176.195.13	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
23.96.208.137	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
184.105.139.108	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.46	United States	147.237.76.34	yohalan.idf.il	drop		drop	1
46.121.86.104	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
38.229.1.15	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
66.147.244.138	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
46.117.245.81	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.88	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.219	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
77.201.201.147	France	147.237.0.200	m4u.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.163.68.111	Germany	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
195.66.76.4	Germany	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
2.52.28.35	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
146.185.239.102	Russian Federation	147.237.72.167	ishurim.aka.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
192.243.55.138	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.138	Block	5
192.243.55.137	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.137	Block	4
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	4
192.243.55.136	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.136	Block	3
73.229.45.220	United States	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method [0][0][0]p;[23]œ'OW' [31]]DÂ¹Â°Ã°Ã°mCvÃ°ÃžFÃšÃ, AÂµÃŸÃ¿Ã°Ã²Ã.../Ã°Ãšr_iÃ; [2]]bRÃ~IÃŸÃ¼ [30]]Ã>KhvÃ-ÃŸÃ° [6]]Ã?Ã°Ã·} [11]]Ã°Ã-Ã,Ã?Ã±	Block	1
40.77.167.24	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/milluim/index	Block	1
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/dover/site/mainpage.asp	Block	1
192.243.55.133	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sites/klali/default.asp?siteid=43314&catid=43385&docid=46887&list=1	Block	1
73.229.45.220	United States	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	1
184.105.139.68	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to 147.237.77.243/	Block	1
45.79.10.124		147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to /	Block	1
213.163.66.185	Netherlands	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/news/news.in.aspx	Block	1
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.134	Block	1
73.229.45.220	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Method [0][0][0]p;[23]œ'OW' [31]]DÂ¹Â°Ã°Ã°mCvÃ°ÃžFÃšÃ, AÂµÃŸÃ¿Ã°Ã²Ã.../Ã°Ãšr_iÃ; [2]]bRÃ~IÃŸÃ¼ [30]]Ã>KhvÃ-ÃŸÃ° [6]]Ã?Ã°Ã·} [11]]Ã°Ã-Ã,Ã?Ã±	Block	1
192.243.55.137	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
184.105.247.195	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
66.249.78.4	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1273-he/atal.aspx	Block	1
192.243.55.134	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mpm	Block	1
73.229.45.220	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in URL	Block	1
192.243.55.129	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1
66.249.78.11	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1275-he/atal.aspx	Block	1
73.229.45.220	United States	147.237.76.42	refuah.idf.il	NULL Character in Method [0][0][0]p;[23]œ'OW' [31]]DÂ¹Â°Ã°Ã°mCvÃ°ÃžFÃšÃ, AÂµÃŸÃ¿Ã°Ã²Ã.../Ã°Ãšr_iÃ; [2]]bRÃ~IÃŸÃ¼ [30]]Ã>KhvÃ-ÃŸÃ° [6]]Ã?Ã°Ã·} [11]]Ã°Ã-Ã,Ã?Ã±	Block	1
37.187.114.171	France	147.237.72.156	aman.idf.il	Unauthorized URL Access to /irj/portal	Block	1
208.115.113.84	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/homepage/	Block	1
192.243.55.131	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=59333&docid=68025	Block	1
192.243.55.136	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/kadatz	Block	1