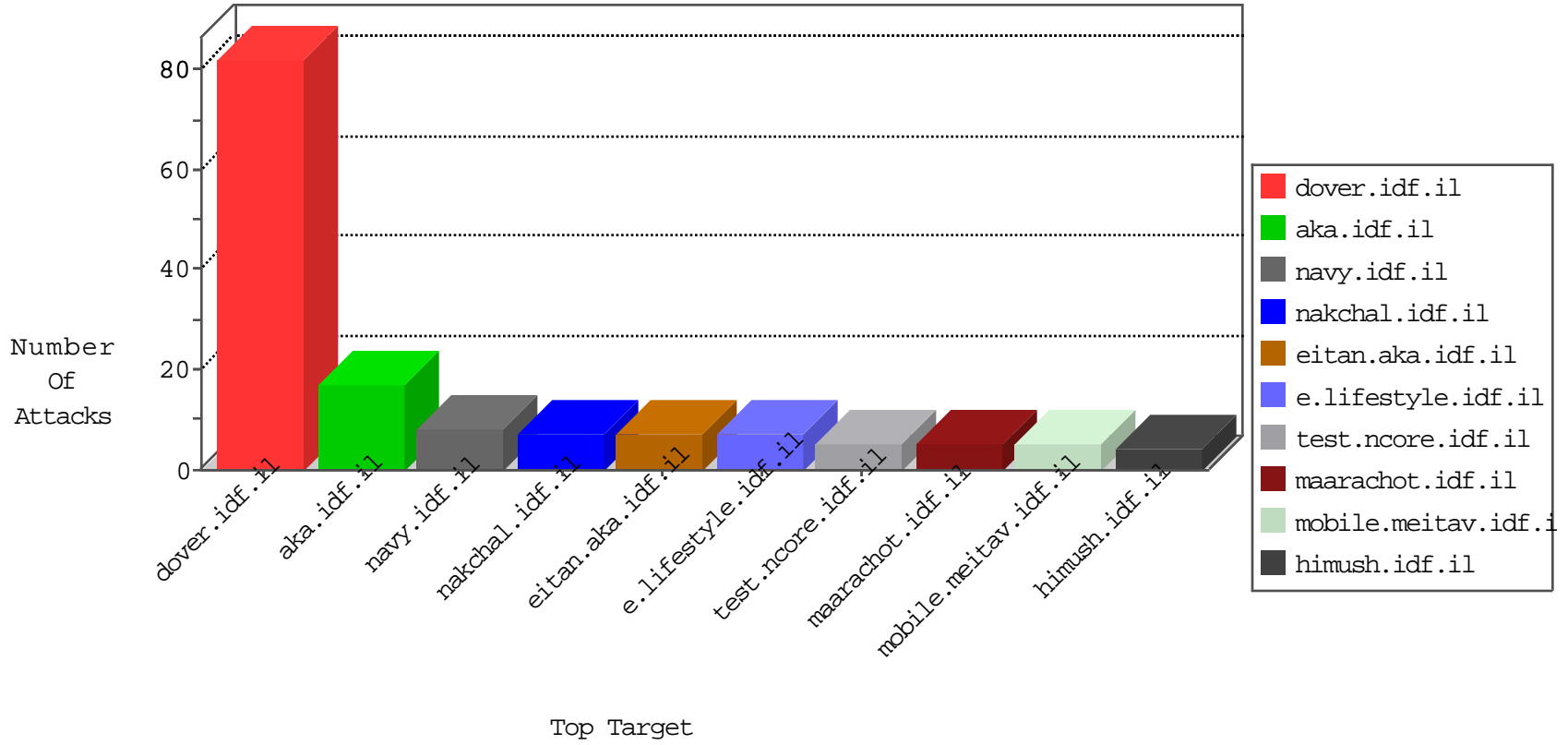


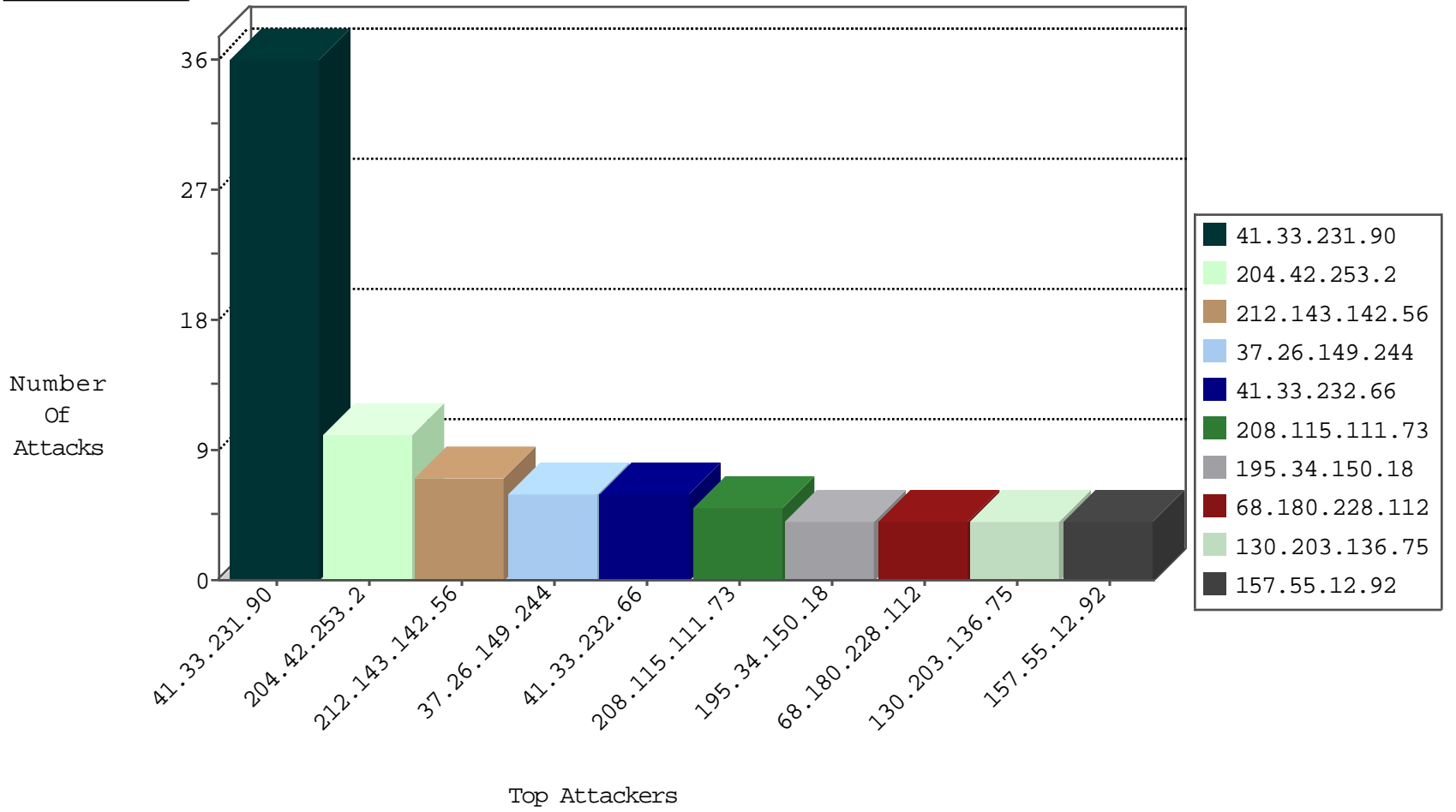
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.42.253.2	United States	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.34	yochalan.idf.il	Block_Ntp_All_Net	drop	2
158.130.6.191	United States	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
58.97.111.9	Thailand	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	1
142.54.160.213	United States	147.237.77.74	law.idf.il	block-sp-traf1	drop	1
1.199.115.141	China	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.246		147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
58.97.111.10	Thailand	147.237.76.86	navy.idf.il	Invalid TCP Flags	drop	1
142.54.160.214	United States	147.237.76.30	himush.idf.il	block-sp-traf1	drop	1
1.199.115.141	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.246		147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
74.91.28.59	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	drop	1
142.54.160.214	United States	147.237.76.86	navy.idf.il	block-sp-traf1	drop	1
1.199.115.141	China	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.246		147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
88.150.177.186	United Kingdom	147.237.76.176	test.noore.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.248.227.164	Slovakia	147.237.77.216	dover.idf.il	21073: HTTP: Fareit/Pony Loader User-Agent	Block	1
188.165.15.211	France	147.237.76.30	himush.idf.il	C228: HTTP: AhrefBot crawler	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	36
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
157.55.12.92	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
31.210.187.236	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
130.203.136.75	United States	147.237.77.216	dover.idf.il	drop	SAM rule	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
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
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.146	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
81.169.237.146	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	2
54.160.159.53	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
37.26.149.244	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
67.220.158.56	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
208.115.111.73	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	2
37.26.149.244	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		alert	2
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
68.180.228.112	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
141.212.122.135	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
139.162.200.97	Netherlands	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
208.115.111.73	United States	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	1
81.169.237.146	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	1
184.105.139.106	United States	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.116.179.250	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.154	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.26.149.244	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.72	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
108.16.231.44	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
195.62.53.168	Russian Federation	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
71.6.135.131	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
146.185.239.102	Russian Federation	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.136	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
31.210.186.100	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.71	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.111.73	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
184.105.139.106	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.154	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.73	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
74.82.47.40	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.85.106	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.140	United States	147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.71	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
81.169.237.146	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	1
184.105.247.224	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
54.191.164.152	United States	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
141.212.122.155	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.26.149.244	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	1
141.212.122.134	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.70.69.213	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/ru	Block	2
54.183.1.75	United States	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/grapheat.stm)	Block	1
41.130.180.60	Egypt	147.237.0.15	kosher-kravi.idf.il	PHP Attempt	Block	1
160.177.249.184		147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
54.183.1.75	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/wp-login.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
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
41.130.180.60	Egypt	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to kosher-kravi.idf.il/xmlrpc.php	Block	1
162.243.175.76	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-en/www.idf.il/english	Block	1
62.0.103.156	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
207.46.13.88	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
52.53.245.71	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
184.105.139.70	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
66.249.65.223	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1381-he/dover.aspx	Block	1
92.113.138.36	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/kapatz/undefined	Block	1
54.67.22.27	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
184.105.247.196	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
160.177.249.184		147.237.76.42	refuah.idf.il	PHP Attempt	Block	1