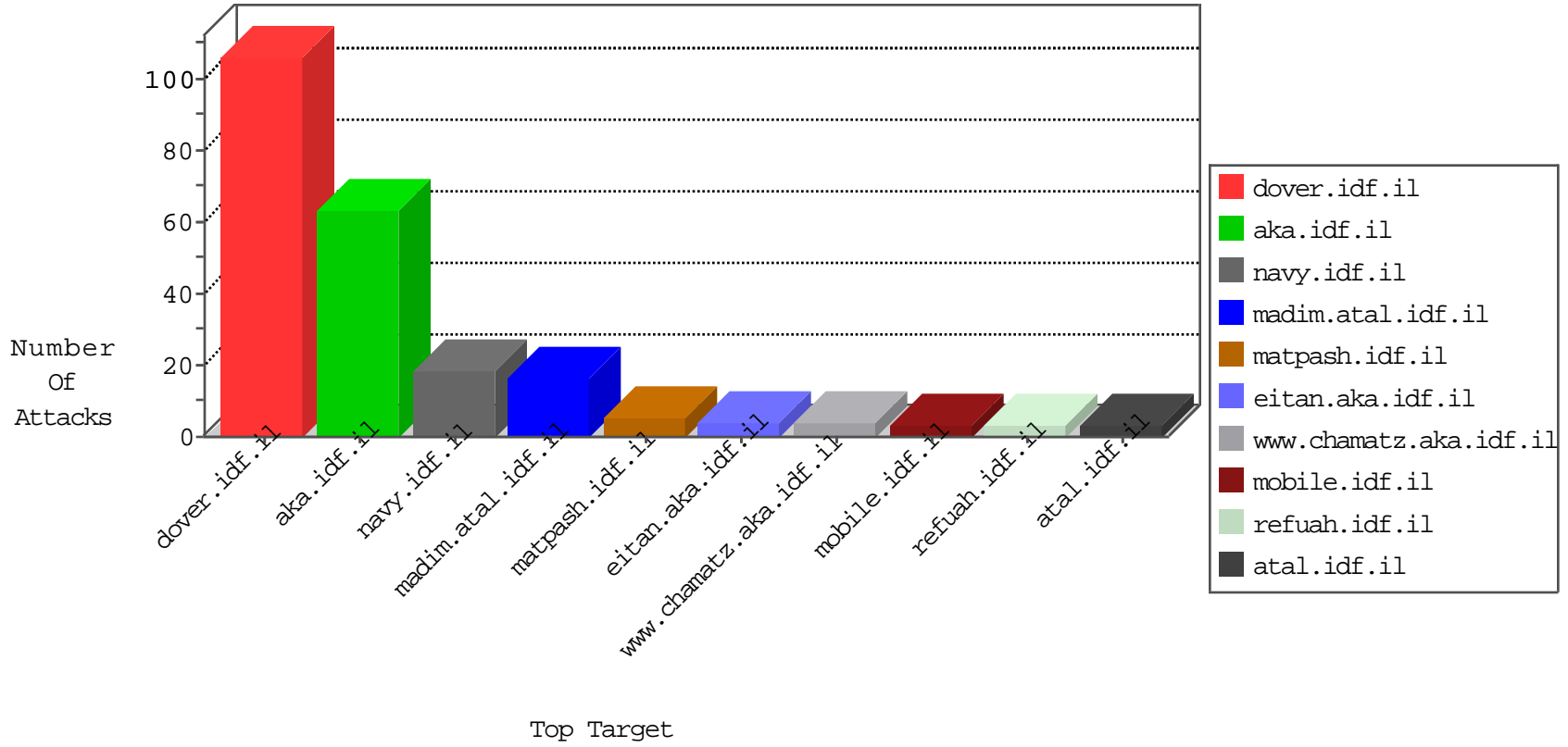




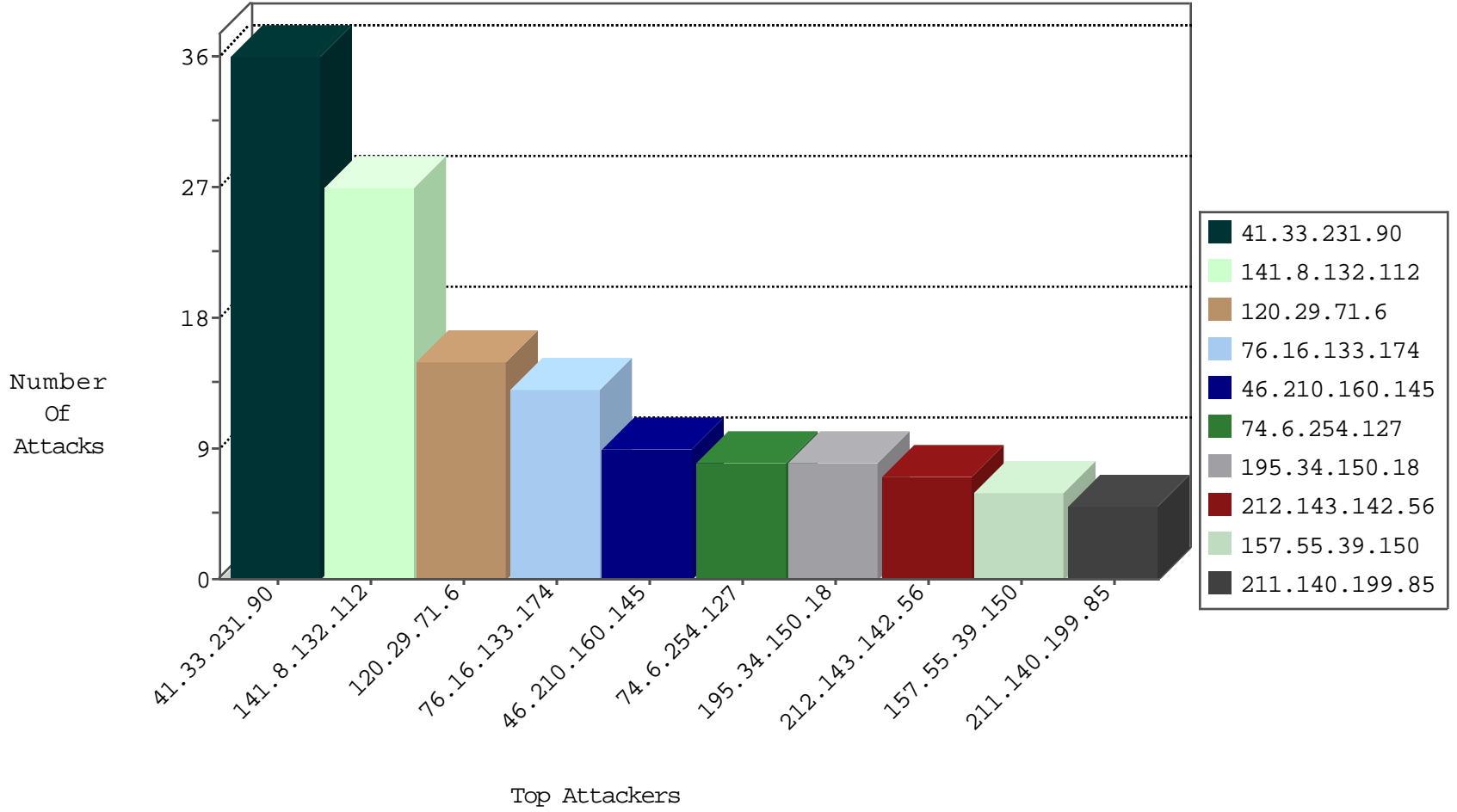
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
58.218.185.120	China	147.237.0.200	m4u.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
188.138.17.205	France	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	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
146.185.250.105	147.237.72.14	Russian Federation	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
94.102.48.193	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.185.120	147.237.77.216	China	dover.idf.il	ET SCAN Potential SSH Scan	1
211.140.199.85	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
211.140.199.85	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
185.72.179.1	147.237.77.233		atal.idf.il	ET SCAN NMAP -f -sS	1
94.102.51.30	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
85.93.5.65	147.237.77.226	Germany	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
58.218.185.120	147.237.76.34	China	yochalan.idf.il	ET SCAN Potential SSH Scan	1
211.140.199.85	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
211.140.199.85	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
211.140.199.85	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
185.72.179.1	147.237.77.233		atal.idf.il	ET SCAN NMAP -sS window 2048	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
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
76.16.133.174	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
74.6.254.127	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
157.55.39.150	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
85.64.122.228	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.24	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.183.34.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.131.51	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.81	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.97.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.191.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
207.46.13.37	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
5.102.195.67	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
157.55.39.218	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
89.163.150.79	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
46.19.85.100	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
138.134.192.10	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
67.85.18.22	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
101.108.20.41	Thailand	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.33	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.22.131.51	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
139.102.165.213	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
207.46.13.59	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.139.103	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
108.54.241.51	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
79.183.206.1	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.79	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
195.62.53.168	Russian Federation	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.44	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.139.104	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
108.54.241.51	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
82.81.193.82	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
198.1.101.123	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
5.78.190.179	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
146.185.239.102	Russian Federation	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
99.239.212.63	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
218.22.211.69	China	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
184.105.247.211	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
115.230.124.164	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
84.108.175.124	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
61.135.169.23	China	147.237.77.216	dover.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
5.78.190.179	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
99.239.212.63	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
218.22.211.69	China	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
188.120.154.159	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.210.160.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
120.29.71.6	Philippines	147.237.76.86	navy.idf.il	PHP Attempt	Block	7
120.29.71.6	Philippines	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 120.29.71.6	Block	6
66.249.66.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	4
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
149.78.222.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed 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
85.64.224.149	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
2.54.187.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
115.239.212.65	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
203.137.80.193	Japan	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/old/wp-admin/	Block	1
66.249.79.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/jquery.nyromodal-1.6.2.js	Block	1
149.78.222.175	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
115.239.212.67	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
207.46.13.111	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.111	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
157.55.39.115	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
115.239.212.69	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1379-he/dover.aspx	Block	1
120.29.71.6	Philippines	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/phpmoadmin/moadmin.php	Block	1
195.159.233.44	Norway	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 195.159.233.44 (Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE))	None	1
115.239.212.138	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
66.249.79.228	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/scroller/jquery.jcarousel.js	Block	1
132.162.125.200	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
195.159.233.44	Norway	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE)	None	1
120.29.71.6	Philippines	147.237.76.86	navy.idf.il	Admin Blocking	Block	1
66.249.79.235	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery.plugins/jquery.scrollfollow.js	Block	1