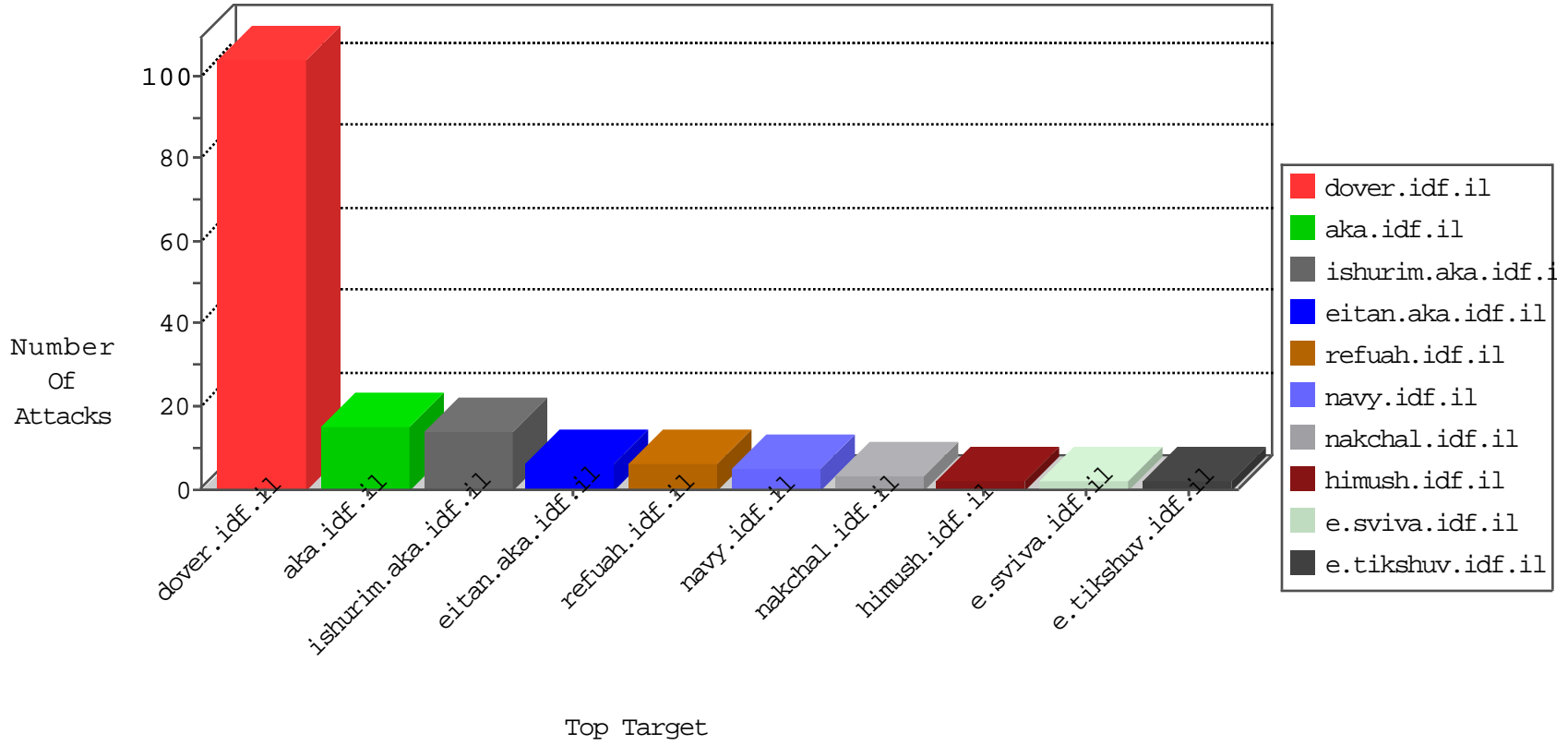


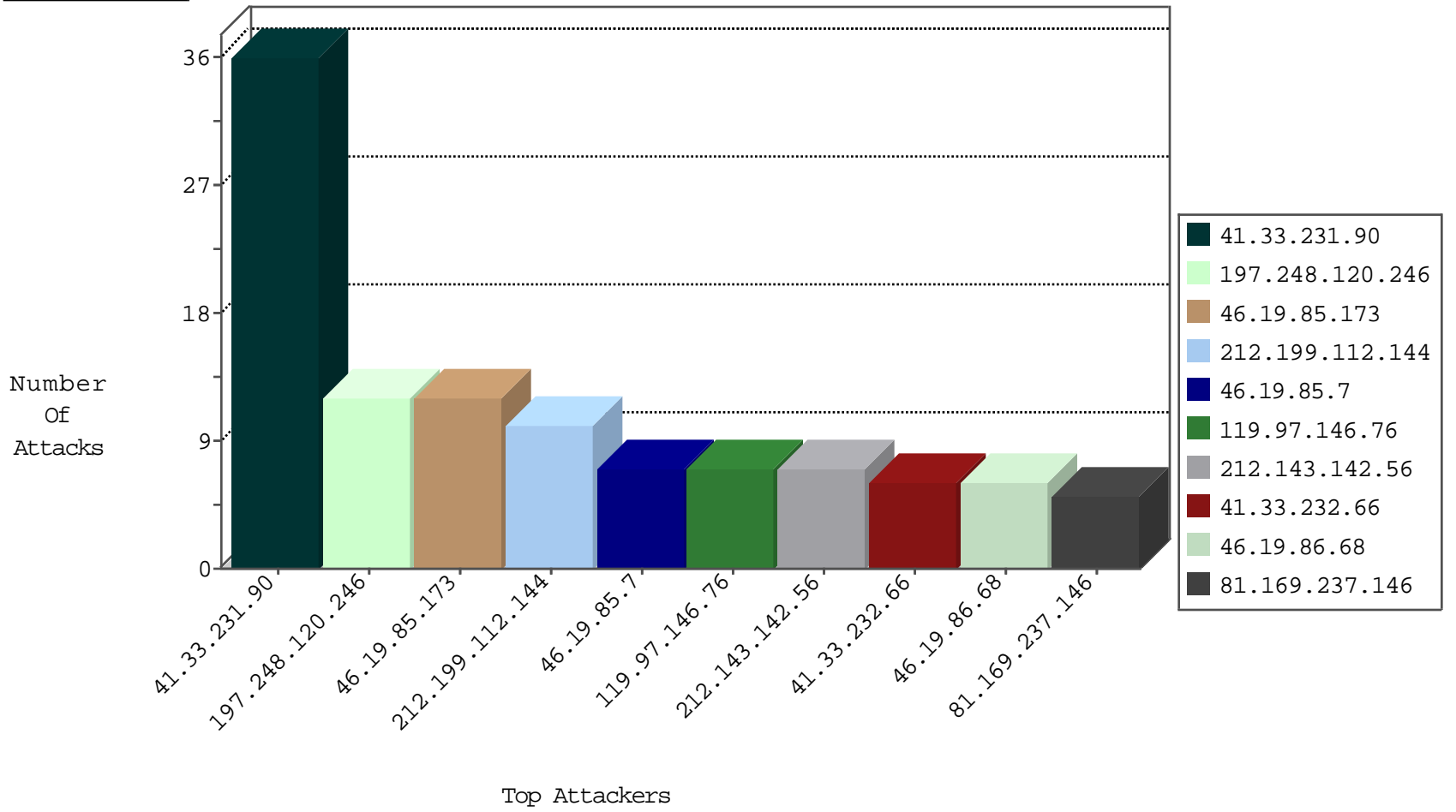
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.199.112.144	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	100
192.118.64.213	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
78.31.65.132	Germany	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.201		147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	1
78.31.65.132	Germany	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
54.67.38.74	United States	147.237.76.200	eitan.aka.idf.il	DOS-httpdx-hreadrequest-FS	dest-reset	1
78.31.65.132	Germany	147.237.76.34	yochalan.idf.il	Block_Udp_All_Nets	drop	1
54.67.38.74	United States	147.237.77.235	sviva.idf.il	DOS-httpdx-hreadrequest-FS	dest-reset	1
185.130.5.201		147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
119.97.146.76	China	147.237.77.216	dover.idf.il	20086: HTTP: Muieblackcat Security Scanner	Block	5
119.97.146.76	China	147.237.77.216	dover.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
151.80.31.110	Italy	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
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
201.172.80.102	147.237.72.14	Mexico	dover.idf.il(old)	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
174.37.194.144	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sA (2)	1
174.37.194.144	147.237.8.27	United States	e.madim.atal.idf.i	ET SCAN NMAP -sA (2)	1
104.128.144.131	147.237.76.199	Canada	e.nakchal.idf.il	ET SCAN NMAP -sS window 3072	1
209.126.116.147	147.237.76.44	United States	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
174.37.194.144	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sA (2)	1
119.97.146.76	147.237.77.216	China	dover.idf.il	ET WEB_SERVER Muieblackcat scanner	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
197.248.120.246	Kenya	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.173	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.173	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	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
46.19.85.7	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.86.4	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.68	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.86.68	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
178.154.189.201	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.78.130	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
188.29.165.101	United Kingdom	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
157.55.39.31	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
66.249.78.245	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.7	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
81.169.237.146	Germany	147.237.77.61	e.oogat.idf.il	drop	SAM rule	drop	2
47.16.116.102	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
66.249.65.251	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
184.105.247.216	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.174	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
104.130.78.65	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	147.237.8.46	e.chiruch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.162	United States	147.237.0.35	akaws.idf.il	drop		drop	1
81.169.237.146	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	1
2.52.130.234	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
123.125.71.26	China	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	1
184.105.139.124	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.162	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
81.169.237.146	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	1
2.52.130.234	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
174.37.194.144	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
123.125.71.26	China	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.28	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.247.199	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.163	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
130.193.51.91	Russian Federation	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
74.82.47.43	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
184.105.247.200	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.173	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.25.43.94	Germany	147.237.0.33	idf.il	drop		drop	1
184.105.139.104	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.161	United States	147.237.0.35	akaws.idf.il	drop		drop	1
81.169.237.146	Germany	147.237.8.46	e.chiruch.idf.il	drop	SAM rule	drop	1

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.182.23.182	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct113\$ct101\$ct103\$cb1Questi on\$76 in aka.idf.il/main/gyus/questionnaire.aspx	None	1
137.99.229.183	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
27.154.224.210	China	147.237.0.17	m.my-kosher-kravi.i df.il	Unauthorized URL Access to 147.237.0.17/getnews.action	Block	1
89.248.174.4	Netherlands	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
183.250.164.156	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/getnews.action	Block	1
66.249.78.245	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter searchText in eitan.aka.idf.il/1002-en/eitan.aspx	None	1
89.248.174.4	Netherlands	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
184.38.201.148	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
191.96.101.34	Chile	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/iraq/english/info09.asp	Block	1
112.198.103.114	Philippines	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 112.198.103.114 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
198.136.53.139	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1