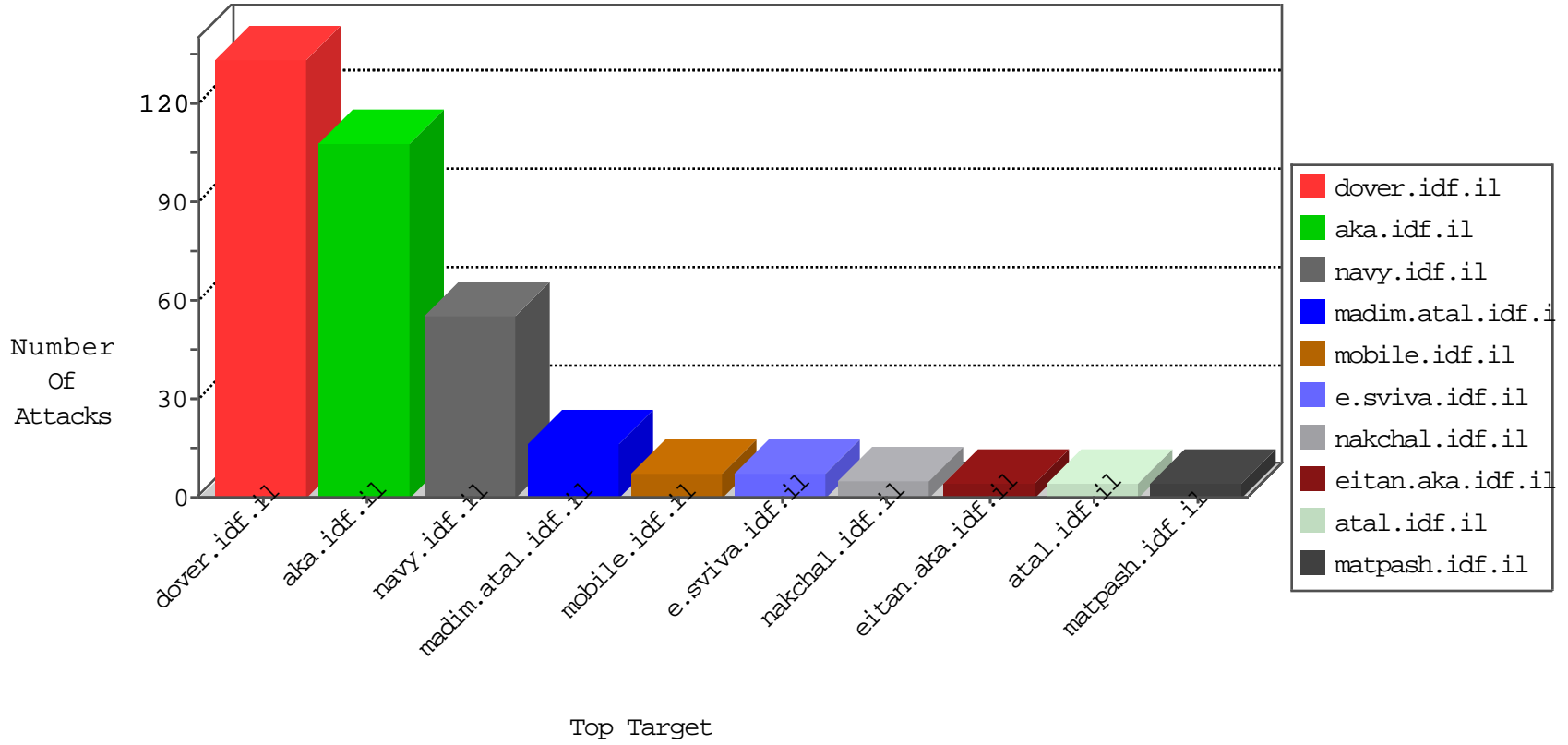


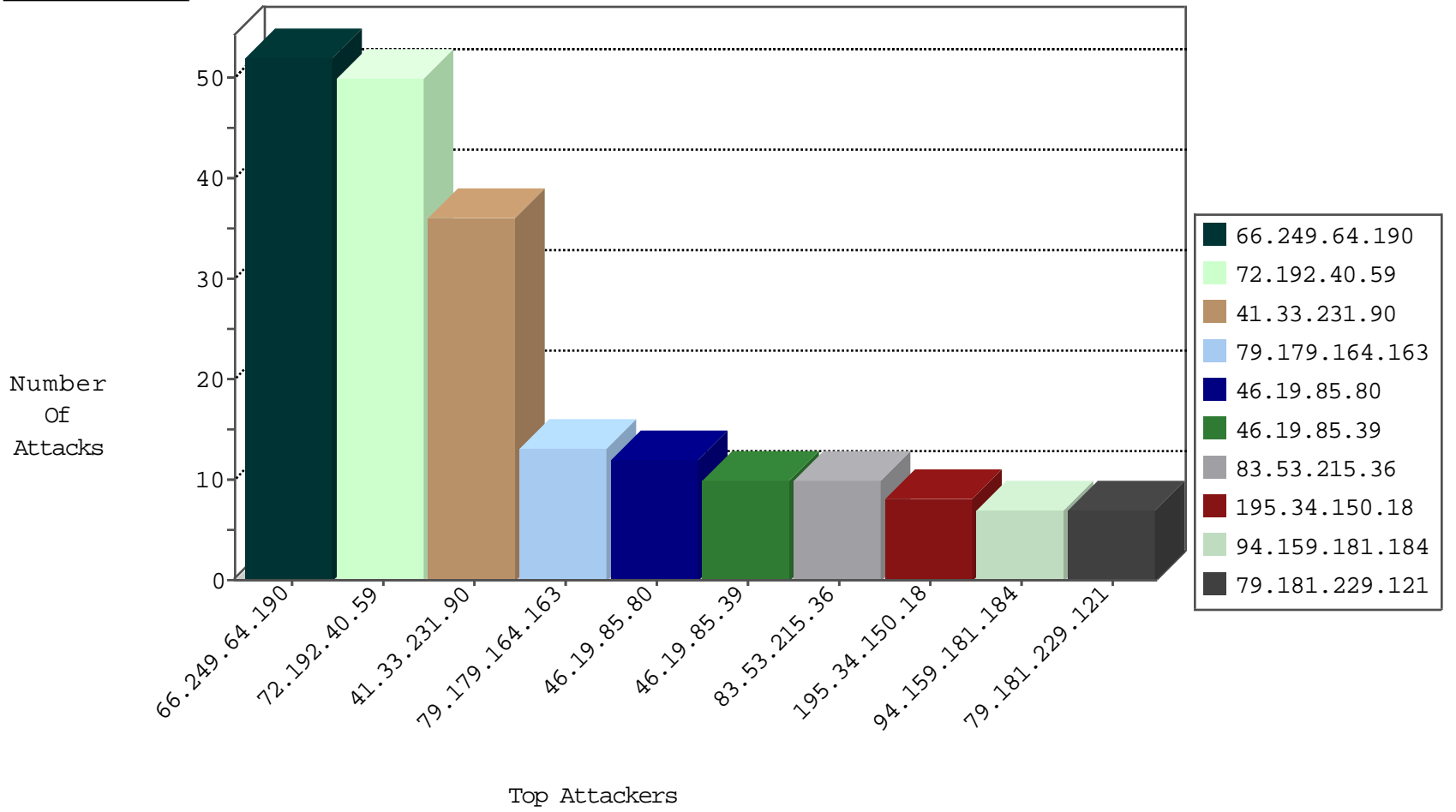
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.82.78.39	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
80.82.78.39	Netherlands	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	1
82.145.33.11	United Kingdom	147.237.76.196	e.sviva.idf.il	Block_Ip_Web_In	drop	1
80.82.78.39	Netherlands	147.237.76.30	himush.idf.il	Block_Ntp_All_Net	drop	1
89.163.132.132	Germany	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

01-27-2016-01:07:51 to 01-27-2016-02:07:51

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.59.60.67	France	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.64.190	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	50
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
109.253.145.162	147.237.77.216	Israel	dover.idf.il	GPL SCAN myscan	2
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
109.253.145.162	147.237.77.216	Israel	dover.idf.il	INDICATOR-SCAN myscan	2
194.187.249.120	147.237.76.39	Europe	mobile.meitav.idf.il	ET SCAN NMAP -sS window 3072	1
54.179.135.126	147.237.76.196	Singapore	e.sviva.idf.il	ET SCAN NMAP -sS window 4096	1
194.187.249.120	147.237.76.39	Europe	mobile.meitav.idf.il	ET SCAN NMAP -sS window 4096	1
82.117.208.243	147.237.72.14		dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
54.179.135.126	147.237.76.196	Singapore	e.sviva.idf.il	ET SCAN NMAP -sS window 3072	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
72.192.40.59	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	50
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
83.53.215.36	Spain	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
46.19.85.80	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
94.159.181.184	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.229.121	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.80	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
46.19.85.39	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.105	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.26.148.148	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.39	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
203.219.134.86	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
109.186.2.38	Israel	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
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
94.230.86.189	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.94.197.174	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.231.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.148.25	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.126.86.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
157.55.39.215	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.211	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.52.53.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
73.69.15.72	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
46.19.85.215	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
73.69.15.72	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.219	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
46.19.85.219	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
66.249.78.160	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
128.232.110.28	United Kingdom	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
46.19.86.6	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.215	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
85.64.95.174	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
176.13.26.224	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
8.37.227.68	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
141.212.122.170	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.117.126.138	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
128.232.110.28	United Kingdom	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
195.60.232.57	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.213	United States	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.166	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
46.19.86.77	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
109.10.175.222	France	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
85.65.110.184	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
176.13.26.224	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
31.210.187.158	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.171	United States	147.237.0.19	madim.atal.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
79.179.164.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
79.179.164.163	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$txtStreet in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	3
85.65.43.147	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
40.77.167.89	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 40.77.167.89	Block	2
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1824-he/dover.aspx	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
40.77.167.91	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-15982-he/dover	Block	1
109.66.126.171	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 109.66.126.171	Block	1
79.181.229.121	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
64.251.25.176	United States	147.237.72.166	aka.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	None	1
151.80.31.153	Italy	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
94.159.181.184	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/	Block	1
46.19.85.61	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
109.66.126.171	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/1/size338x0/1541.jpg	Block	1
79.182.199.203	Israel	147.237.76.31	nakchal.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$ucFaqControl\$txtSearch in www.nakchal.idf.il/1072-he/nakchal.aspx	Block	1
64.251.25.176	United States	147.237.72.166	aka.idf.il	Multiple signatures from 64.251.25.176	Block	1
199.46.199.231	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/us	Block	1
94.230.86.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.61	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
141.212.122.160	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
79.182.199.203	Israel	147.237.76.31	nakchal.idf.il	Parameter Type Violation search in www.nakchal.idf.il/1072-he/nakchal.aspx	Block	1
66.249.65.174	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-9067-he/atal.aspx	Block	1
207.241.226.230	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/application/http	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.19.85.61	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
141.212.122.160	United States	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training/transportation.asp	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.180.151.106	Israel	147.237.72.166	aka.idf.il	Multiple Untraceable SSL Sessions from 79.180.151.106 (Unknown SSL Session)	None	1
46.19.86.147	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$ct138\$ct101\$ct103\$cb1Question\$3 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
141.212.122.160	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	1
85.65.87.249	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1