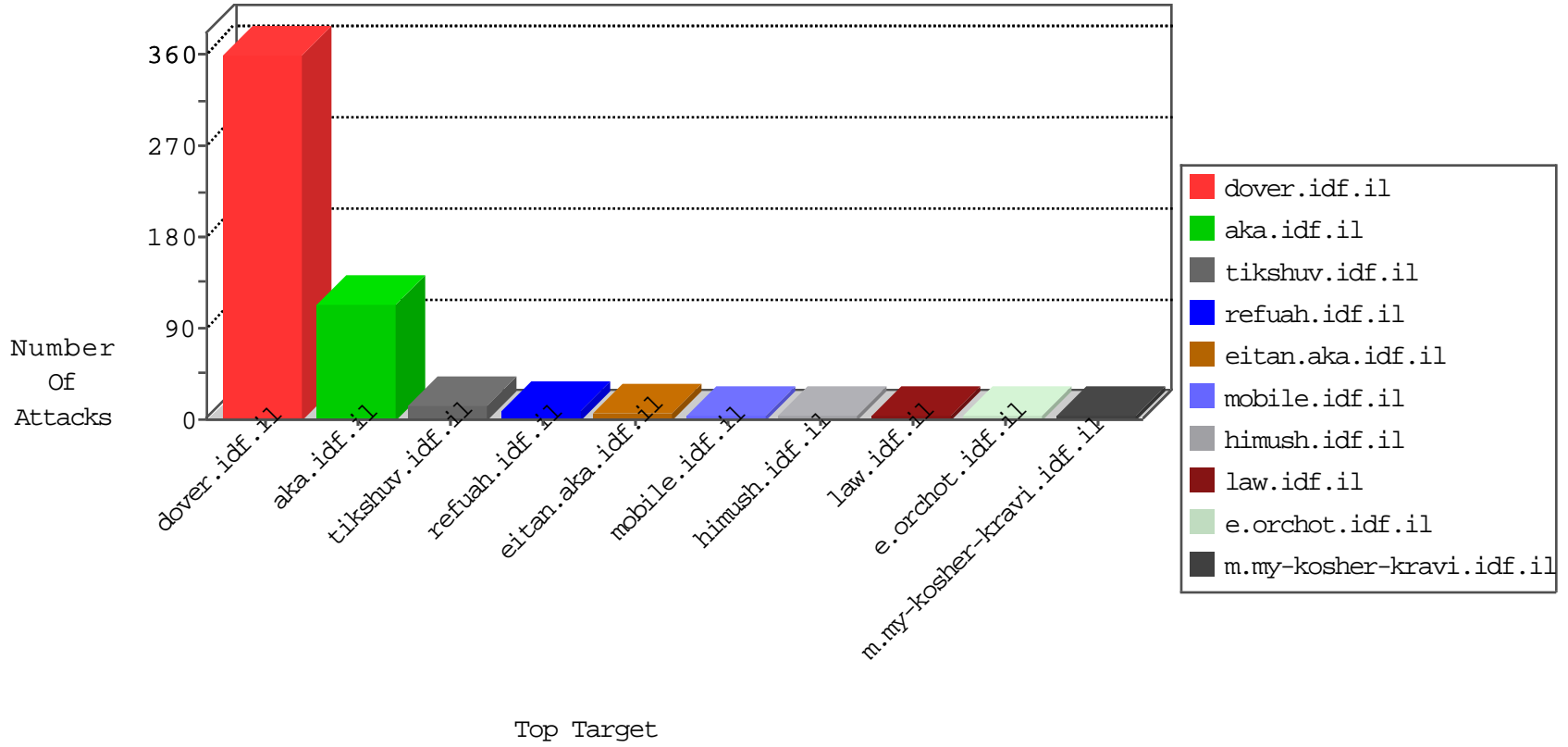


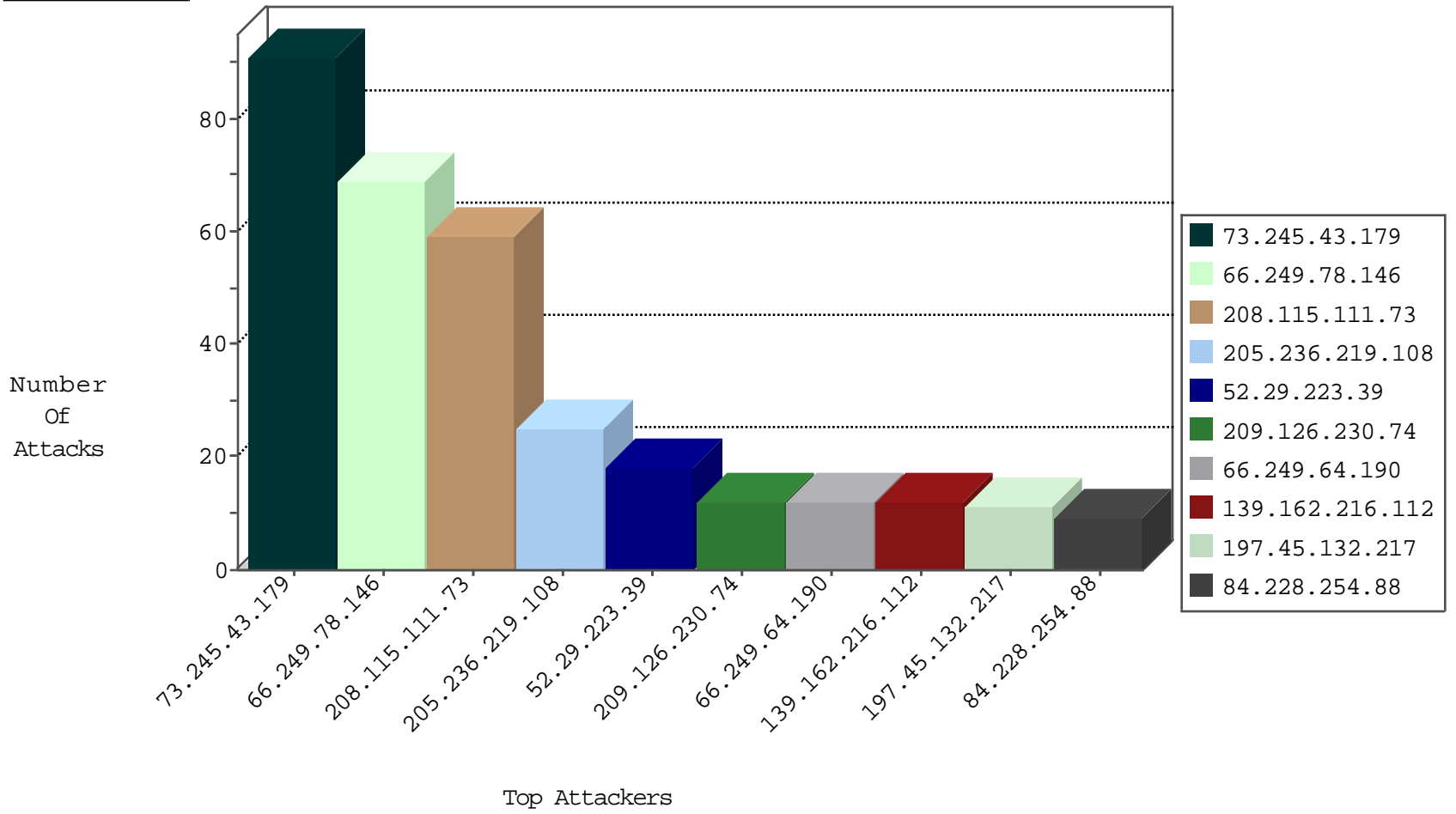
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.65.210	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
80.82.78.38	Netherlands	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	2
50.207.42.93	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	2
104.131.108.100	United States	147.237.76.42	refuah.idf.il	Block_Ntp_All_Net	drop	1
209.126.136.2	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
94.102.49.116	Netherlands	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
73.42.76.220	United States	147.237.76.148	ggcenter.aka.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
180.201.32.5	China	147.237.72.166	aka.idf.i	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
70.82.118.4	147.237.77.216	Canada	dover.idf.il	Xenu Link Sleuth User Agent	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.66.23	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
183.60.48.25	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
177.33.145.171	147.237.0.34	Brazil	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
107.158.255.194	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 3072	1
104.214.29.239	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 2048	1
80.82.78.38	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.230.74	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 1024	1
68.116.21.226	147.237.8.50	United States	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.230.74	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.48.25	147.237.76.42	China	refuah.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
107.158.255.194	147.237.77.176	United States	matpash.idf.il	ET SCAN NMAP -sS window 4096	1
104.219.238.10	147.237.72.217	United States	e.idf.il	ET SCAN NMAP -sS window 1024	1
104.214.29.239	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -f -sS	1
209.126.230.74	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.78.158	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
201.172.161.45	147.237.8.14	Mexico	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
193.201.227.120	147.237.0.34	Ukraine	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
73.245.43.179	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	90
66.249.78.146	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	69
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
205.236.219.108	Canada	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	25
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
139.162.216.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
197.45.132.217	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
84.228.254.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
203.87.27.234	Australia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
68.180.231.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
50.167.125.92	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
66.249.78.199	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.16.5.197	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
207.46.13.137	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
50.87.144.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
216.145.14.142	United States	147.237.0.34	tikshuv.idf.il	Header Rejection	header rejection pattern found in request	monitor	4
207.46.13.2	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
157.55.39.134	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
192.249.66.247	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
52.10.0.89	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
178.154.189.8	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.90.106	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
73.235.247.61	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
66.249.78.230	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.64.177	United States	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.93.245	Europe	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
118.160.133.92	Taiwan	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
50.110.235.57	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
95.220.215.64	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
8.37.70.77	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
72.106.70.221	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
199.30.24.26	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
64.236.82.3	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
118.160.133.92	Taiwan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
45.35.64.142	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
52.87.232.15	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
118.160.133.92	Taiwan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
157.55.39.204	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
141.212.122.147	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
51.255.65.97	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
88.191.204.49	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
193.124.248.122	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
5.29.213.220	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
74.82.47.50	United States	147.237.77.121	e.navy.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
128.72.24.220	Russian Federation	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/general.aspx	Block	1
66.249.78.158	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in tikshuv.idf.il/site/gallery.aspx	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
52.21.178.185	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1519-en/dover.aspx#.any	Block	1
151.80.31.168	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
70.82.118.4	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation docId in tikshuv.idf.il/site/story.aspx	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
66.249.64.230	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 178.255.215.87	Block	1
76.90.162.228	United States	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
2.53.34.220	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct113 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
216.218.206.66	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19485-he/kkkkkkkk=23f25da9kkkkkkk_23f25da9	Block	1
80.82.78.38	Netherlands	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.baidu.com/cache/global/img/gs.gif	Block	1
5.29.191.129	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1302	Block	1
217.23.14.168	Netherlands	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
109.67.141.82	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
66.249.78.104	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/7/112387.pdf	Block	1
207.46.13.137	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter SearchText in www.eitan.aka.idf.il/938-he/eitan.aspx	None	1
5.29.213.220	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1