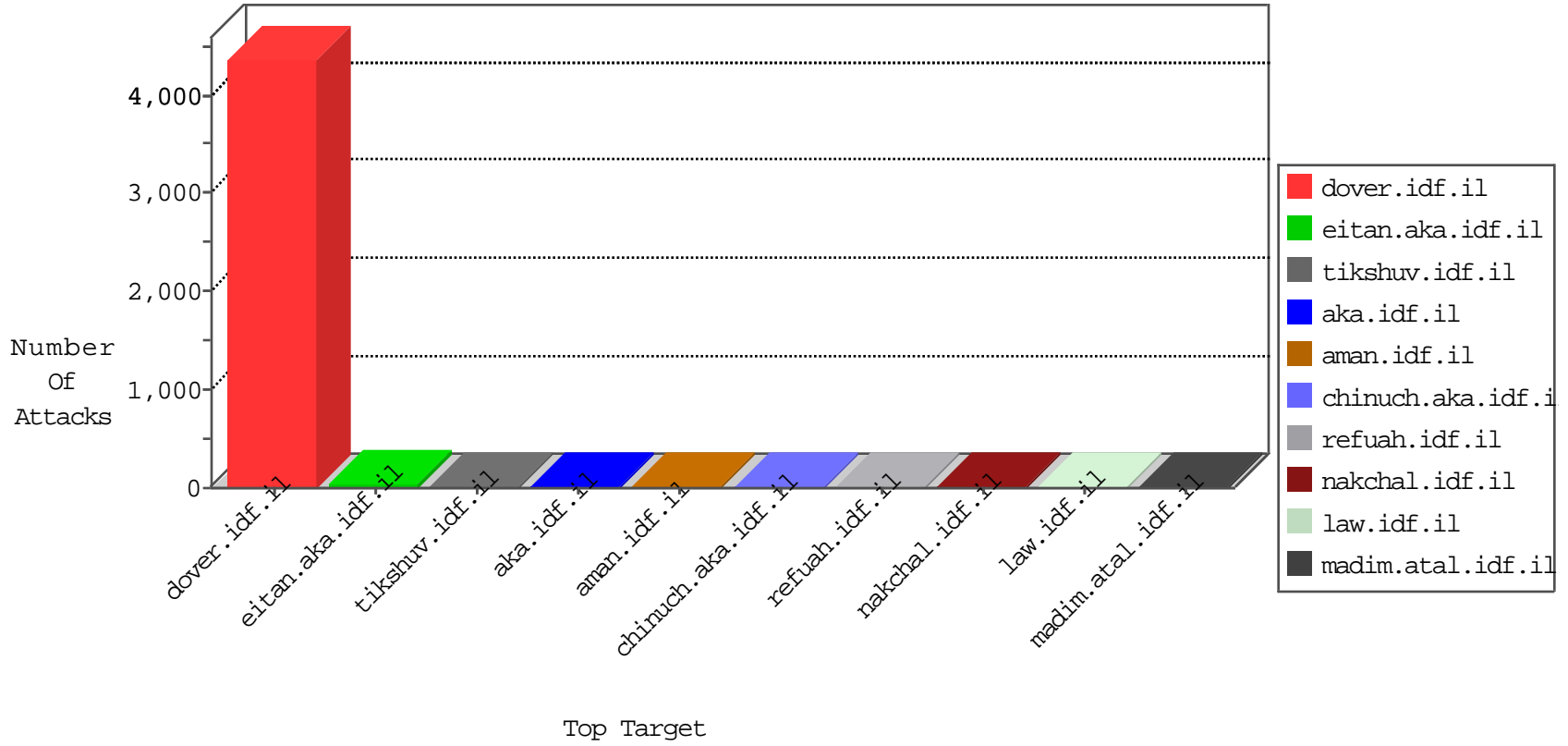




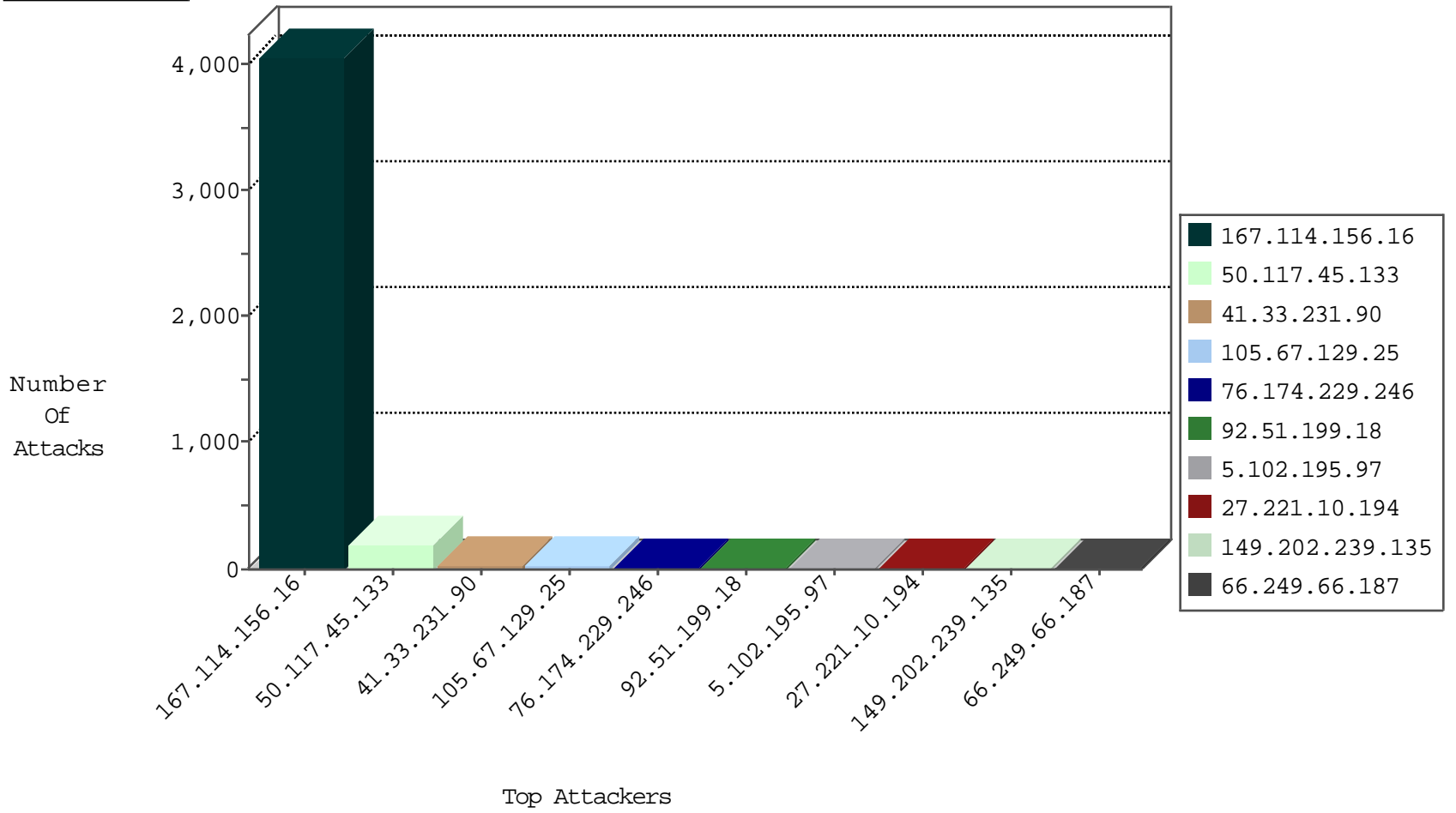
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4061
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
159.122.220.135	United States	147.237.77.121	e.navy.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	1
159.122.220.135	United States	147.237.0.200	m4u.idf.il	Block_Ntp_All_Net	drop	1
185.103.252.96	Russian Federation	147.237.77.74	law.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.120.173.103	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
66.249.66.187	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
66.249.66.190	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

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
27.221.10.194	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
209.114.36.145	147.237.76.42	United States	refuah.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
27.221.10.194	147.237.76.34	China	yohalan.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	147.237.76.199	United States	e.nakchal.idf.il	ET DROP Dshield Block Listed Source	1
13.94.233.163	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 3072	1
193.201.227.117	147.237.0.33	Ukraine	idf.il	ET SCAN Potential SSH Scan	1
13.94.233.163	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -f -sS	1
112.203.215.95	147.237.76.31	Philippines	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
106.186.113.67	147.237.72.166	Japan	aka.idf.il	ET SCAN NMAP -sS window 1024	1
104.238.82.190	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
27.221.10.194	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
27.221.10.194	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
223.4.174.30	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
27.221.10.194	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
204.152.218.49	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
27.221.10.194	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
13.94.233.163	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 2048	1
162.144.41.122	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
106.186.113.67	147.237.77.61	Japan	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
106.184.2.29	147.237.76.177	Japan	ncore.idf.il	ET SCAN Potential SSH Scan	1
27.221.10.194	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
27.221.10.194	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
50.117.45.133	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	198
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
76.174.229.246	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
92.51.199.18	Ireland	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
105.67.129.25	Morocco	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
5.102.195.97	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
66.249.66.187	United States	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.5.3	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.147.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
105.67.129.25	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.117.182.13	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	5
132.70.66.12	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.53.132.11	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.255.215.87	France	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.79.31	United States	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
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
105.67.129.25	Morocco	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
105.67.129.25	Morocco	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
31.25.77.7	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	2
141.212.122.204	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
31.210.187.30	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
162.144.41.122	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.91	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
50.117.45.133	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
195.60.232.57	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.205	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.80	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
89.138.83.152	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
40.78.146.128	United States	147.237.77.216	dover.idf.il	Instant Messengers	instant messenger pattern found, application: Skype	monitor	1
162.144.41.122	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.95	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.205	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.87	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.204	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
218.22.211.69	China	147.237.76.34	yohalan.idf.il	drop		drop	1
141.212.122.205	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.88	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.204	United States	147.237.8.50	e.tikshuv.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
70.211.67.124	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
157.55.39.12	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.90	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
194.187.168.212	France	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.202.239.135	France	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1283-en/dover.aspx parameter PageNum	Block	6
149.202.239.134	France	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1283-en/dover.aspx	Block	6
2.53.174.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
40.77.167.1	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
149.202.239.134	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-15344-he/dover.aspx	Block	1
208.115.113.82	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/unselecatble.aspx	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.78.236	Block	1
2.53.166.208	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakchal.idf.il/templates/general/mobile	Block	1
209.114.36.145	United States	147.237.76.42	refuah.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
141.212.122.81	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to /x	Block	1
54.210.18.124	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
149.202.239.135	France	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.78.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/3382.jpg	Block	1
141.212.122.81	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to /x	Block	1
54.210.18.124	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
177.19.188.29	Brazil	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/templates/navmenu/navmenu.css.aspx	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/4/size100x0/3424.jpg	Block	1
27.159.234.88	China	147.237.77.176	matpash.idf.il	Unauthorized HTTP Method	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8921-he/refuah.aspx	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/sendtofriend/mmmmmmm=7a4abce2mmmmmm_7a4abce2	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1379-he/dover.aspx	Block	1
40.77.167.1	United States	147.237.77.216	dover.idf.il	Abnormally Long Request URL	Block	1