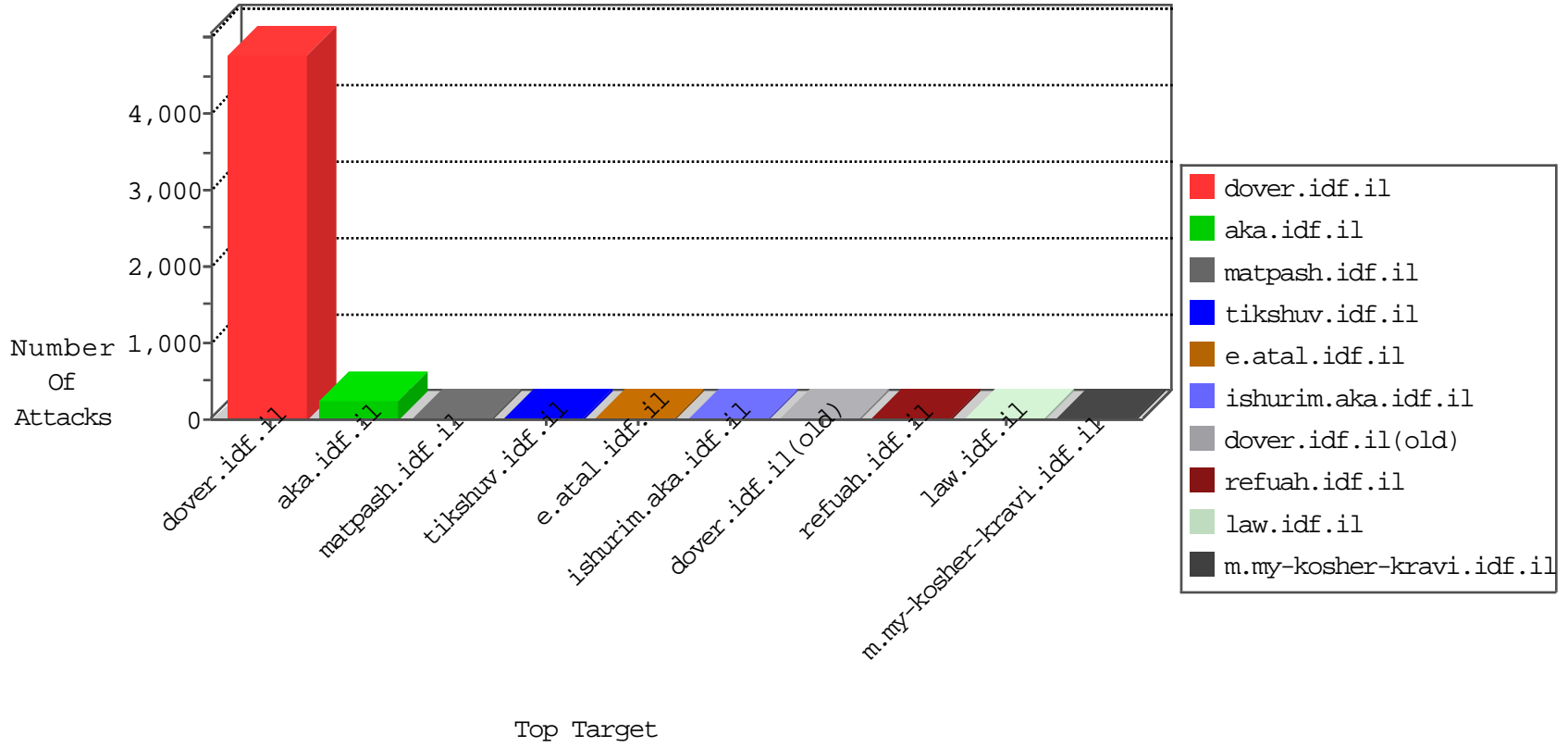


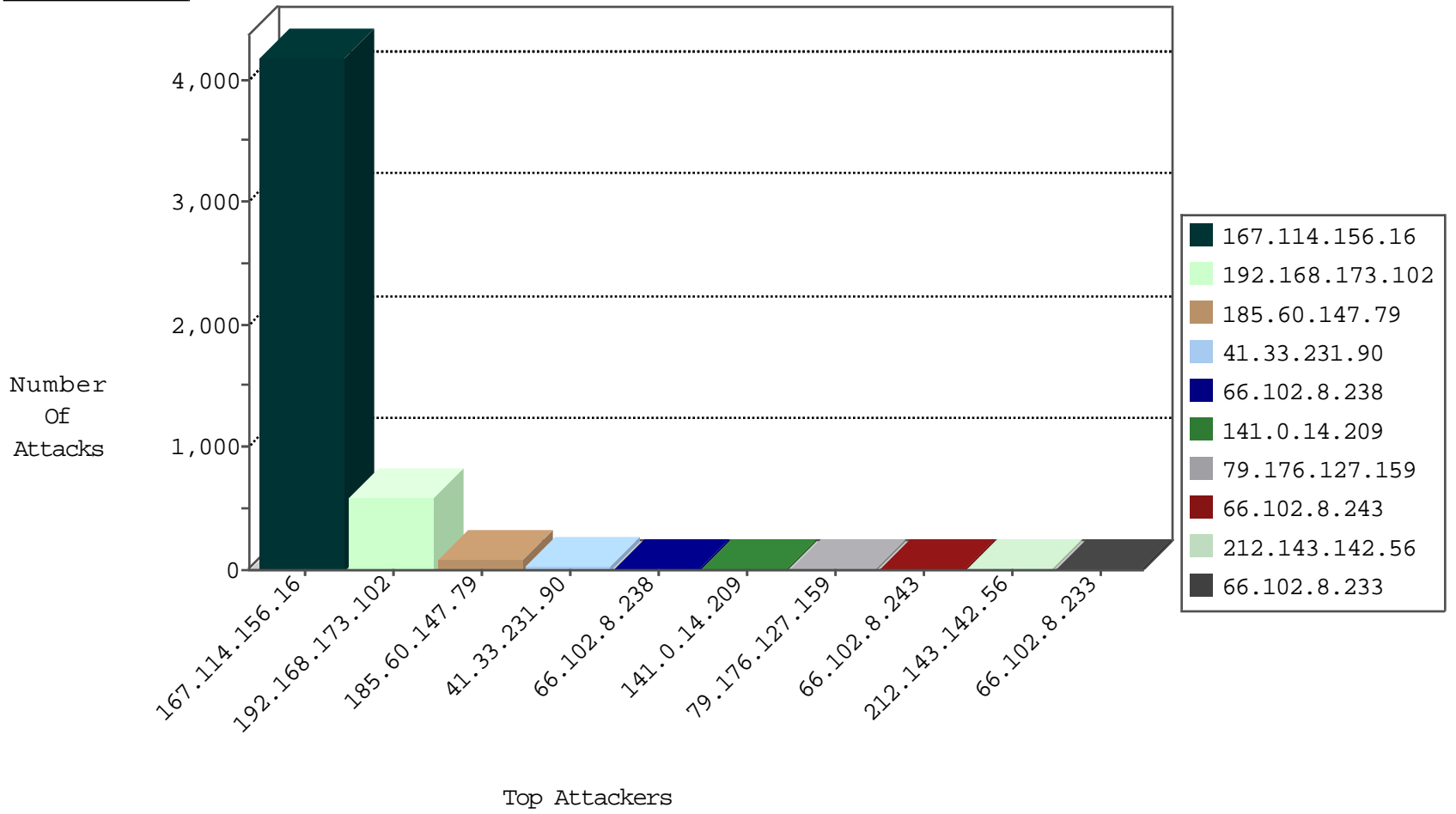
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.60.147.79	Switzerland	147.237.77.216	dover.idf.il	TCP Scan (vertical)	drop	15993
167.114.156.16	Canada	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	4161
204.42.253.2	United States	147.237.72.14	dover.idf.il(old)	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.0.15	kosher-kravi.idf.il	Block_Ntp_All_Net	drop	2
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
192.3.220.210	United States	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	1
192.3.220.210	United States	147.237.77.205	prisha.idf.il	Block_Udp_All_Nets	drop	1
216.218.206.83	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.246	Lithuania	147.237.77.170	maarachot.idf.il	Block_Ntp_All_Net	drop	1
204.42.253.2	United States	147.237.0.19	madim.atal.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.121.112.142	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
149.202.47.161	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
149.202.47.161	France	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
157.55.2.161	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
207.46.13.45	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.78.120	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
66.249.69.34	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
104.128.144.131	147.237.77.212	Canada	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.78.38	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
210.117.121.60	147.237.76.197	Korea, Republic of	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
209.87.255.117	147.237.0.34	Canada	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
179.43.144.37	147.237.76.30	Switzerland	himush.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243	147.237.8.14		e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
210.117.121.60	147.237.76.197	Korea, Republic of	e.himush.idf.il	ET SCAN NMAP -sS window 3072	1
209.87.255.117	147.237.0.35	Canada	akaws.idf.il	ET SCAN Potential SSH Scan	1
209.87.255.117	147.237.0.17	Canada	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	375
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	205
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
141.0.14.209	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
79.176.127.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	9
185.3.147.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.169.243.32	Germany	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
119.122.247.60	China	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
172.56.18.93	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
178.255.215.87	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
91.108.88.84	Germany	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
41.107.8.89	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
2.52.140.223	Israel	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
141.212.122.169	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
119.122.247.60	China	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
79.176.127.159	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
186.15.186.83	Costa Rica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
31.39.188.171	France	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
165.132.62.117	Korea, Republic of	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.116	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.113.84	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
41.107.8.89	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
185.106.92.47	Russian Federation	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.173	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
79.176.127.159	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.125	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
95.38.61.199	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
41.254.2.72	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
185.106.92.47	Russian Federation	147.237.0.33	idf.il	drop		drop	1
141.212.122.174	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.110	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.126	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
95.38.61.199	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
216.218.206.76	United States	147.237.8.24	e.lifestyle.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
66.240.213.93	United States	147.237.72.14	dover.idf.il(old)	drop	SAM rule	drop	1
185.106.92.47	Russian Federation	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
164.138.23.232	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.111	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
193.163.235.203	Denmark	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
41.107.8.89	Algeria	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.236	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.168	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.106	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
66.249.65.83	Israel	147.237.0.33	idf.il	drop		drop	1
185.106.92.47	Russian Federation	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
164.138.23.232	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.115	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
206.55.101.94	United States	147.237.77.216	dover.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
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
66.249.69.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/gyus/general.aspx	Block	1
87.71.136.171	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
66.249.65.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
66.249.69.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/	Block	2
119.122.247.60	China	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/./shared/usercontrols/headerupper/	Block	1
66.249.66.121	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
66.249.75.44	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	1
66.249.66.123	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/jquery-ui.js	Block	1
68.180.230.155	United States	147.237.76.200	eitan.aka.idf.	Unknown Parameter &SortDir in www.eitan.aka.idf.il/1103-he/eitan.aspx	None	1
41.107.234.196	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
66.249.66.125	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/sa_swfobject.js	Block	1
68.180.231.43	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
50.116.28.209	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1