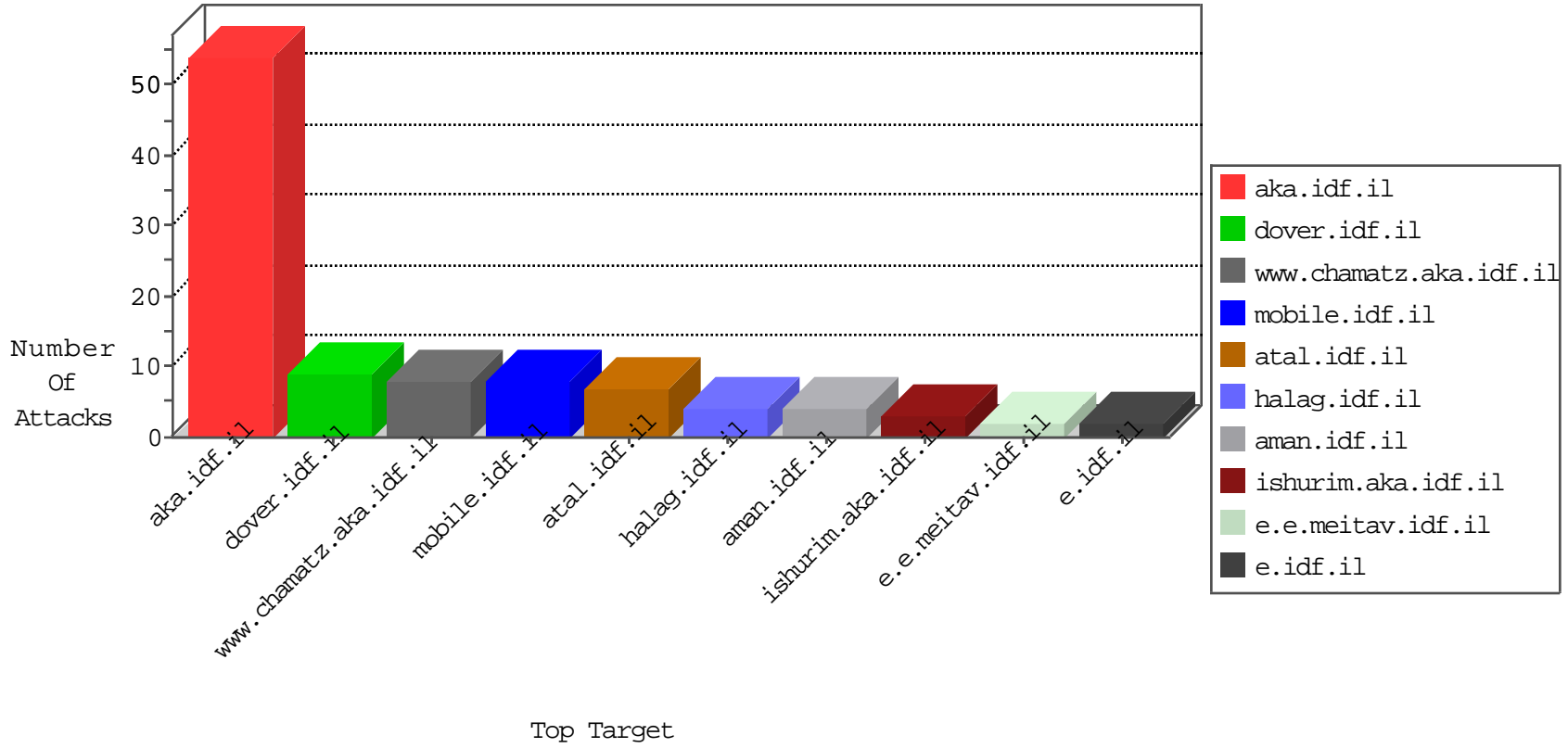


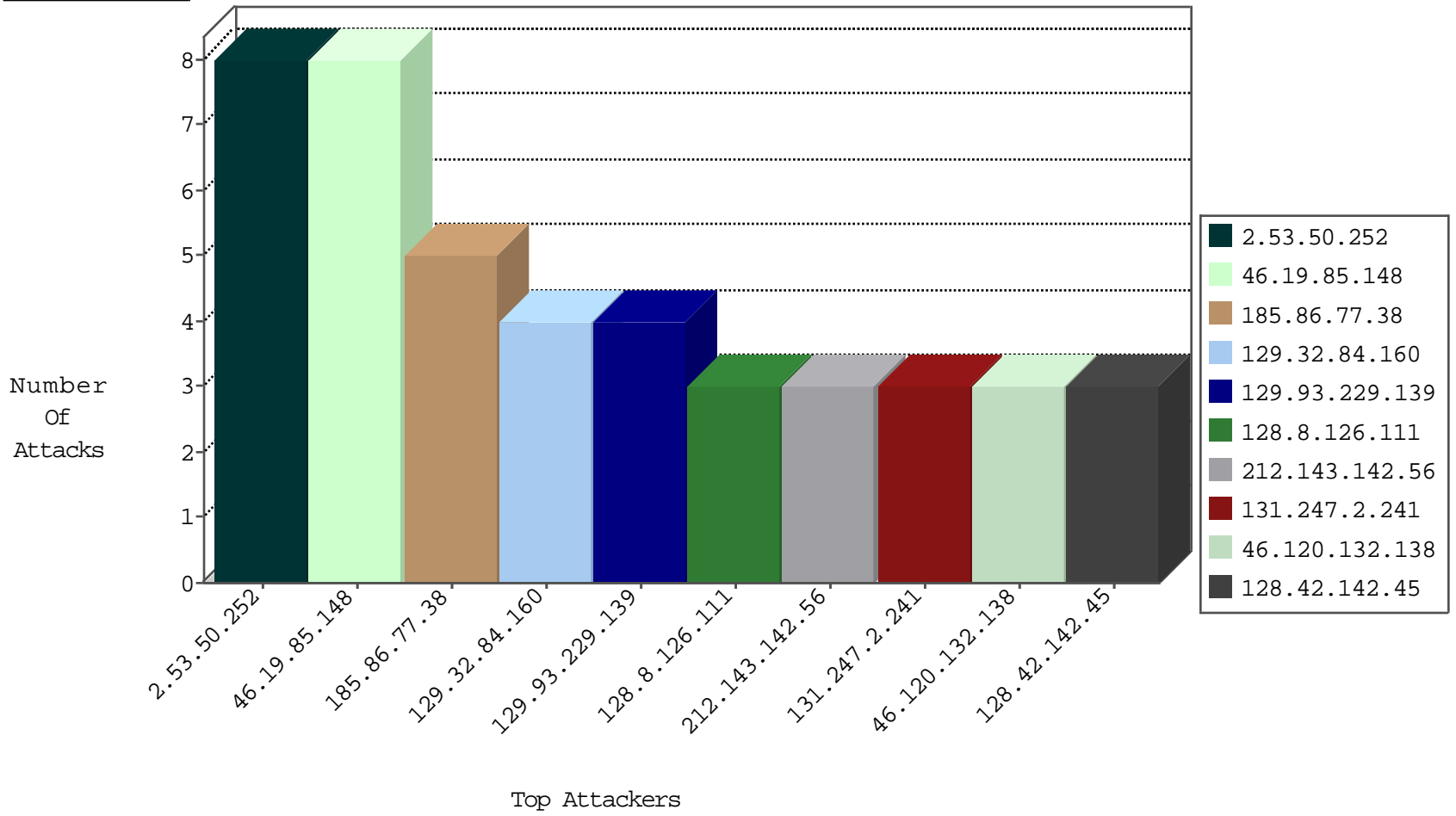
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
134.197.113.3	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
195.113.161.84	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
141.212.113.178	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	2
153.90.1.34	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
198.133.224.147	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
60.166.27.141	China	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.195.4.69	New Zealand	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
0.0.0.0		147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	1
204.85.191.10	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
165.242.90.128	Japan	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
46.185.192.202	Jordan	147.237.77.216	dover.idf.il	network flood IPv4 ICMP	drop	1
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
193.1.13.12	Ireland	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
153.90.1.34	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
134.117.226.180	Canada	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
129.22.150.78	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
60.166.27.141	China	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
194.29.178.13	Poland	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
141.22.213.34	Germany	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
160.80.221.39	Italy	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
134.117.226.180	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
222.45.172.115	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
220.231.195.122	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
177.99.218.218	147.237.77.74	Brazil	law.idf.il	ET SCAN NMAP -sS window 1024	1
154.16.199.218	147.237.77.234	United States	halag.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
220.231.195.122	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 4096	1
194.44.253.106	147.237.77.205	Ukraine	prisha.idf.il	ET SCAN NMAP -sS window 4096	1
154.16.199.218	147.237.77.235	United States	sviva.idf.il	ET SCAN Potential SSH Scan	1
104.154.31.136	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection	1
31.24.228.20	147.237.0.16	United Kingdom	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.19.85.148	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.53.50.252	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
129.10.9.53	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
141.212.122.96	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.120.34.199	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
176.13.225.218	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.97	United States	147.237.76.38	e.e.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.120.132.138	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
138.246.253.19	Germany	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.85.24	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.110	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.120.132.138	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.71	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.111	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
106.38.241.105	China	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
141.212.122.72	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
46.19.85.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
176.13.225.218	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
106.38.241.105	China	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.50.252	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	2
77.139.103.137	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
185.86.77.38	Ukraine	147.237.77.233	atal.idf.il	Parameter Type Violation searchText in www.atal.idf.il/1385-he/atal.aspx	Block	1
46.120.34.199	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
157.55.39.112	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
185.86.77.38	Ukraine	147.237.77.233	atal.idf.il	Parameter Type Violation searchText in www.atal.idf.il/1424-he/atal.aspx	Block	1
46.120.132.138	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
185.86.77.38	Ukraine	147.237.77.74	law.idf.il	Parameter Type Violation pos in www.law.idf.il/163-7423-he/patzar.aspx	Block	1
204.79.180.156	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/default.aspx	Block	1
66.249.76.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
185.86.77.38	Ukraine	147.237.77.233	atal.idf.il	Parameter Type Violation &SortDir in atal.idf.il/1368-he/atal.aspx	Block	1
207.46.13.115	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
69.47.161.8	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/sachar	Block	1
185.86.77.38	Ukraine	147.237.77.233	atal.idf.il	Parameter Type Violation PageNum in atal.idf.il/1368-he/atal.aspx	Block	1