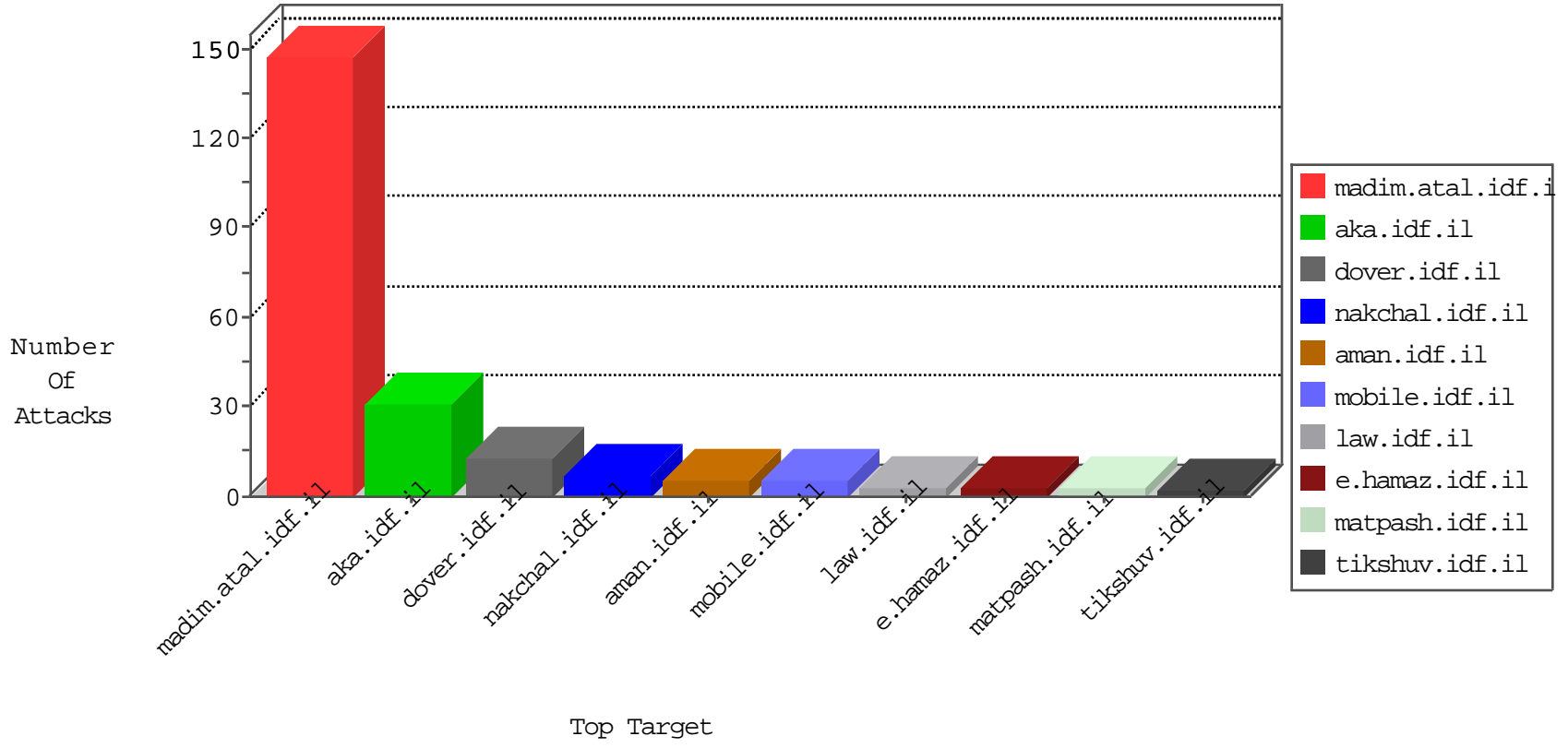


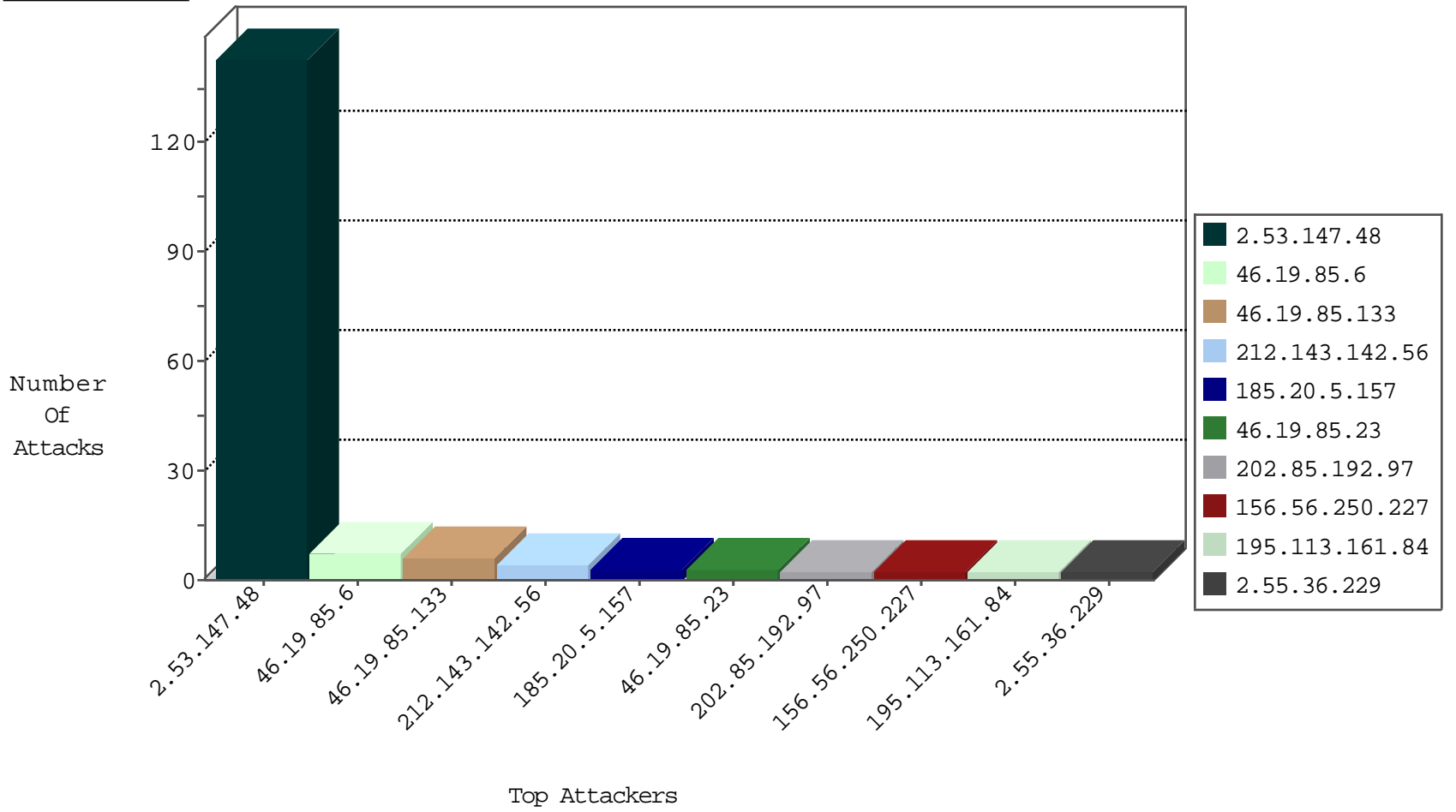
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
156.56.250.227	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
204.85.191.11	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
195.113.161.84	Czech Republic	147.237.72.166	aka.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	1
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
198.82.160.238	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
131.247.2.241	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
141.22.213.34	Germany	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
143.225.229.236	Italy	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.217.77.4	New Zealand	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1

09-16-2016-06:04:07 to 09-16-2016-07:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.174.95.106	Netherlands	147.237.72.167	ishurim.aka.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.121.116.113	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
202.85.192.97	147.237.76.199	Hong Kong	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
133.208.21.66	147.237.0.15	Japan	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
40.121.139.43	147.237.77.227	United States	e.haraz.idf.il	ET SCAN NMAP -sS window 1024	1
202.85.192.97	147.237.77.212	Hong Kong	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
133.208.21.66	147.237.76.30	Japan	himush.idf.il	ET SCAN NMAP -sS window 1024	1
92.29.69.152	147.237.8.27	United Kingdom	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.227.67.158	147.237.77.235	Sweden	sviva.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
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.133	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.6	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.133	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
199.241.27.33	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.6	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.238	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.19.85.6	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
60.225.128.87	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
5.29.156.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
141.212.122.110	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
106.38.241.105	China	147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.100	United States	147.237.72.217	e.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.58	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
31.16.254.235	Germany	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.226.161.155	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
106.186.113.169	Japan	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.105	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
79.176.96.189	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	1
46.19.85.6	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.247.198	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
112.10.194.27	China	147.237.77.74	law.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
141.212.122.106	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
85.65.112.22	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.247.242	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
123.59.54.189	China	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
2.53.178.159	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.109	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
101.178.206.92	Australia	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	1
141.212.122.99	United States	147.237.72.217	e.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
2.53.147.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	143
46.19.85.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
104.128.144.131	Canada	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/redirect.php	Block	1
2.55.36.229	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 2.55.36.229	Block	1
204.79.180.100	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
66.249.66.105	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
124.73.11.123	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-en/matpash.aspx/trackback/	Block	1
2.55.145.187	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
207.46.13.129	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/templates/departmentslobby/	Block	1
66.249.76.72	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/apple-app-site-association	Block	1
128.172.35.27	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/	Block	1
207.46.13.166	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/kamlar/newspaper.asp	Block	1
91.227.71.250	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	1
141.8.132.16	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
46.19.85.133	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	1
217.132.117.177	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/	Block	1
104.128.144.131	Canada	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/redirect.php	Block	1
2.55.36.229	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz/res#012ources/images/innerpage/goback.gif	Block	1
157.55.39.238	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
46.19.86.95	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	1