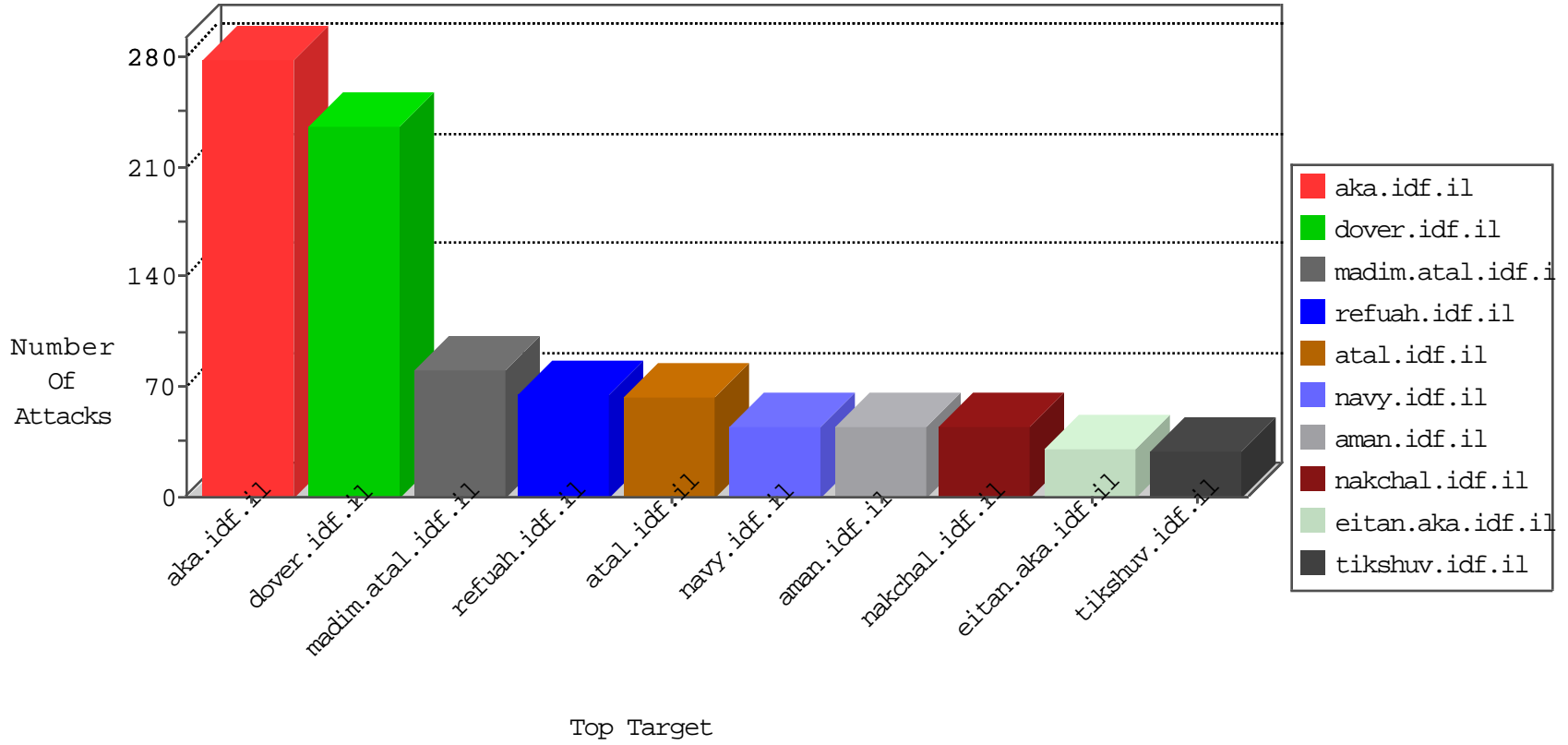


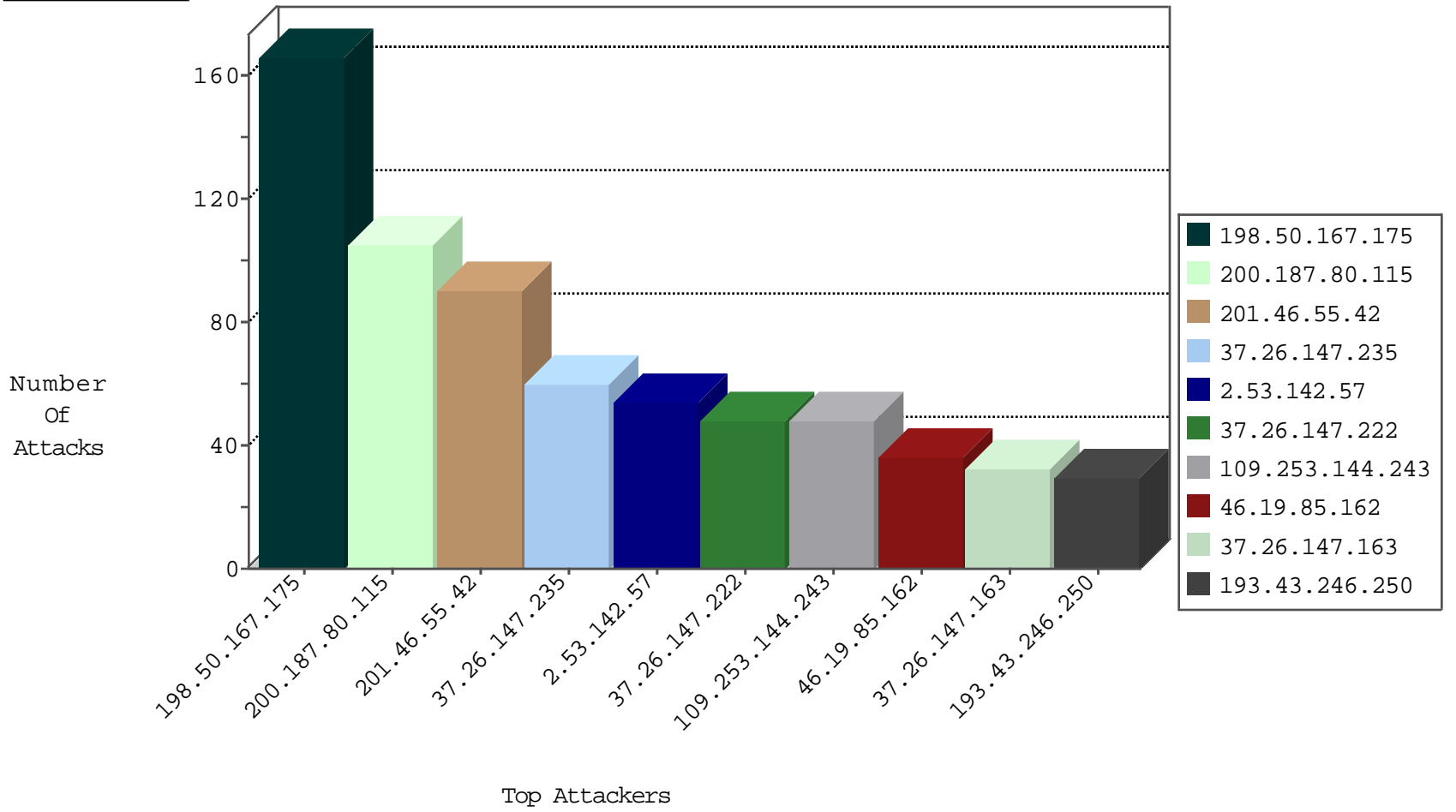
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	6
37.26.147.241	Israel	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	2
120.132.50.135	China	147.237.72.156	anan.idf.il	block-sp-trafl	forward	1
130.217.77.2	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
193.166.167.4	Finland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.82	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-10-2016-23:04:01 to 09-11-2016-00:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
197.231.221.211	Liberia	147.237.77.216	dover.idf.il	24910: HTTP: Python urllib User-Agent Header	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
201.38.68.132	147.237.77.226	Brazil	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
130.237.215.157	147.237.8.24	Sweden	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.8.50	Netherlands	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
130.237.215.157	147.237.76.39	Sweden	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
104.237.146.151	147.237.76.201	United States	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	29
37.26.147.235	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
37.26.147.222	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
2.53.142.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	16
2.53.142.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
2.53.142.57	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
46.19.86.92	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
37.46.41.203	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
37.26.147.235	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
207.46.13.192	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	12
37.26.148.151	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.147.163	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
37.26.147.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
37.26.147.222	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
37.26.147.163	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	10
46.19.85.162	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
141.226.147.158	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
37.26.147.222	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
46.19.85.162	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
198.50.167.175	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
141.226.147.158	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
198.50.167.175	Canada	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
46.19.85.251	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
198.50.167.175	Canada	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
37.26.147.235	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
37.26.147.235	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	9
198.50.167.175	Canada	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
46.19.85.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
198.50.167.175	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
2.53.149.71	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
198.50.167.175	Canada	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
37.26.147.230	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
198.50.167.175	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
198.50.167.175	Canada	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
198.50.167.175	Canada	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
37.26.147.230	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
198.50.167.175	Canada	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
198.50.167.175	Canada	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
46.19.85.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
5.102.195.49	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
198.50.167.175	Canada	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
198.50.167.175	Canada	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
198.50.167.175	Canada	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
139.162.13.205	Singapore	147.237.76.39	mobile.meitav.idf.il	drop	SAM rule	drop	7
198.50.167.175	Canada	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
139.162.13.205	Singapore	147.237.77.233	atal.idf.il	drop	SAM rule	drop	7
198.50.167.175	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
2.53.3.98	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
198.50.167.175	Canada	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
198.50.167.175	Canada	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.144.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
37.26.148.178	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
77.139.163.147	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/sitemap.aspx	Block	6
109.253.213.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.120	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
195.90.103.48	Poland	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.228.192.32	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
85.64.191.205	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
109.253.133.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.176.82.230	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
46.19.86.33	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
37.26.146.172	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/nav.css	Block	1
185.27.106.72	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
93.172.122.35	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00\$ctl00\$cpMain\$cpMain\$ctl25 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.69.96	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1517-he/atal.aspx	Block	1
46.4.22.136	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
79.178.195.120	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.66.167.33	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
66.249.76.72	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/.well-known/assetlinks.json	Block	1
46.19.86.33	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
84.108.118.11	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
46.116.30.203	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 46.116.30.203	Block	1
37.26.148.182	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchildsubcategories/1423	Block	1
109.66.169.55	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
77.138.144.238	France	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.19.86.33	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
2.55.40.57	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
85.64.7.149	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
46.121.252.215	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
37.46.41.203	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1136-he/atal.aspx	Block	1
109.226.45.85	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
46.19.86.33	Israel	147.237.77.216	dover.idf.il	Distributed Unknown HTTP Request Method	Block	1
5.102.195.49	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
176.228.192.32	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.69.92	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
40.77.167.43	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1