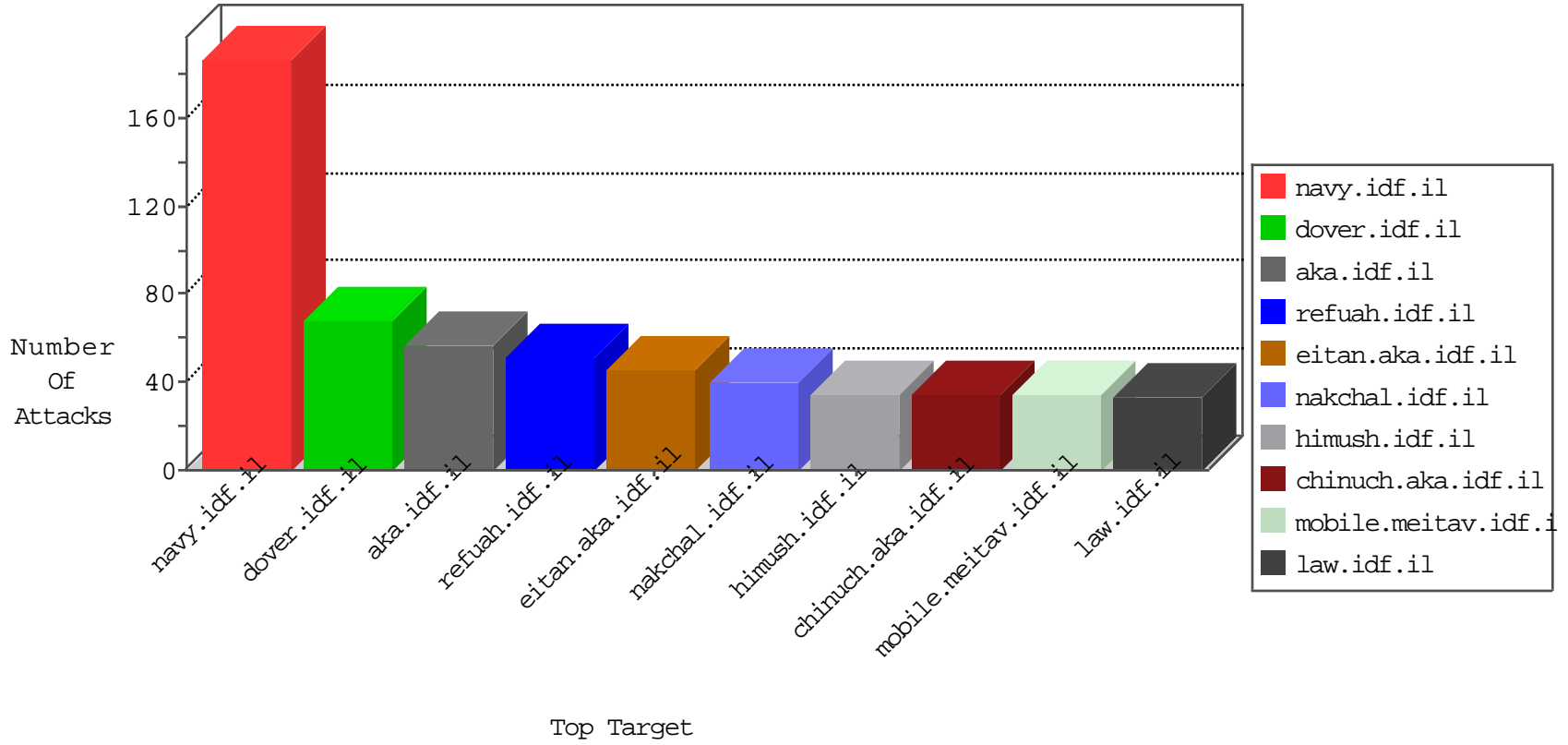


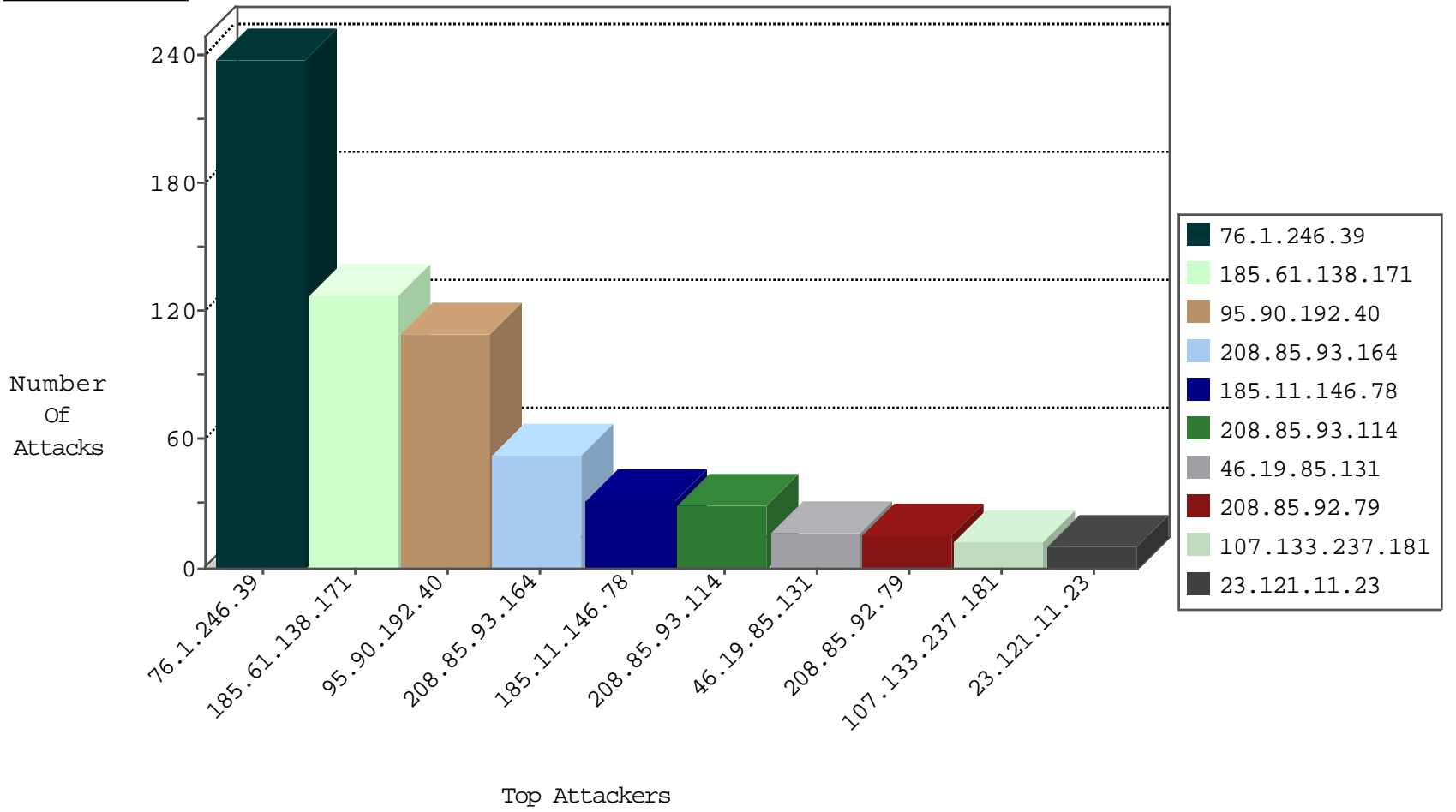
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
204.42.253.130	United States	147.237.76.86	navy.idf.il	Black List	drop	2
61.141.250.97	China	147.237.76.202	e.halag.idf.il	Black List	drop	1
118.112.59.225	China	147.237.76.202	e.halag.idf.il	Black List	drop	1
182.85.57.144	China	147.237.76.202	e.halag.idf.il	Black List	drop	1

09-06-2016-06:04:08 to 09-06-2016-07:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.130	United States	147.237.77.234	halag.idf.il	C1000074: HTTP: majestic bot	Permit	2

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.121.222.79	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	4
84.93.84.77	147.237.77.216	United Kingdom	dover.idf.il	Tehila - Perl LWP with fake user agent	2
45.79.111.169	147.237.72.167	United States	ishurim.aka.idf.il	WEB-MISC Chunked-Encoding transfer attempt	2
91.121.220.181	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
84.93.84.77	147.237.77.74	United Kingdom	law.idf.il	Tehila - Perl LWP with fake user agent	2
37.48.93.217	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
37.48.93.217	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential SSH Scan	1
103.207.37.82	147.237.77.243	Vietnam	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
37.48.93.217	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	1
94.102.52.71	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
12.68.215.78	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.76.200	Ukraine	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
37.48.93.217	147.237.77.227	Netherlands	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
37.48.93.217	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN Potential SSH Scan	1
208.100.26.228	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
37.48.93.217	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
97.105.173.114	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
37.48.93.217	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.50	147.237.76.200	Ukraine	eitan.aka.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.50	147.237.76.200	Ukraine	eitan.aka.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
37.48.93.217	147.237.77.234	Netherlands	halag.idf.il	ET SCAN Potential SSH Scan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
95.90.192.40	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	106
76.1.246.39	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
76.1.246.39	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
76.1.246.39	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
76.1.246.39	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
76.1.246.39	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
76.1.246.39	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
76.1.246.39	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
76.1.246.39	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
185.61.138.171	Ukraine	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
185.61.138.171	Ukraine	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
185.61.138.171	Ukraine	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
107.133.237.181	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
185.61.138.171	Ukraine	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
185.61.138.171	Ukraine	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
185.61.138.171	Ukraine	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
185.61.138.171	Ukraine	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
185.61.138.171	Ukraine	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
46.19.85.167	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	7
23.121.11.23	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.86.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
76.1.246.39	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
76.1.246.39	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
76.1.246.39	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
76.1.246.39	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
76.1.246.39	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
76.1.246.39	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
76.1.246.39	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
76.1.246.39	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.50	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
76.1.246.39	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
76.1.246.39	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.131	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
76.1.246.39	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
76.1.246.39	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.85.131	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
76.1.246.39	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
76.1.246.39	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.85.131	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
66.249.69.251	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
208.85.93.164	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
208.85.93.164	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
185.61.138.171	Ukraine	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
208.85.93.164	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
66.249.76.106	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.61.138.171	Ukraine	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
208.85.93.164	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
208.85.93.164	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.117.17.10	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.132	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
2.55.27.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	2
207.46.13.181	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on ww.idf.il/error.htm	Block	2
76.185.108.254	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for ww.aka.idf.il/ishurim	Block	1
46.19.85.43	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to ww.aka.idf.il/main/	Block	1
176.13.244.231	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
66.249.69.119	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/tizmoret/gallery/	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	1
204.79.180.98	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for ww.aka.idf.il/miluum/templates/home.asp	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
45.79.111.169	United States	147.237.72.167	ishurim.aka.idf.il	Multiple Malformed HTTP Header Line from 45.79.111.169	Block	1
64.62.219.80	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on ww.idf.il/error.htm	Block	1
207.46.13.160	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to ww.my-kosher-kravi.idf.il/	Block	1
66.249.76.81	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
45.79.111.169	United States	147.237.72.167	ishurim.aka.idf.il	Multiple Malformed URL from 45.79.111.169	Block	1
84.95.208.20	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to ww.law.idf.il/templates/general/piwik.php	Block	1
66.249.66.162	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to ww.idf.il/.well-known/assetlinks.json	Block	1
68.180.230.47	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in ww.idf.il/1362-he/dover.aspx	Block	1
45.79.111.169	United States	147.237.72.167	ishurim.aka.idf.il	Multiple Unknown HTTP Request Method from 45.79.111.169	Block	1
89.248.172.16	Netherlands	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/robots.txt	Block	1
66.249.69.93	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1