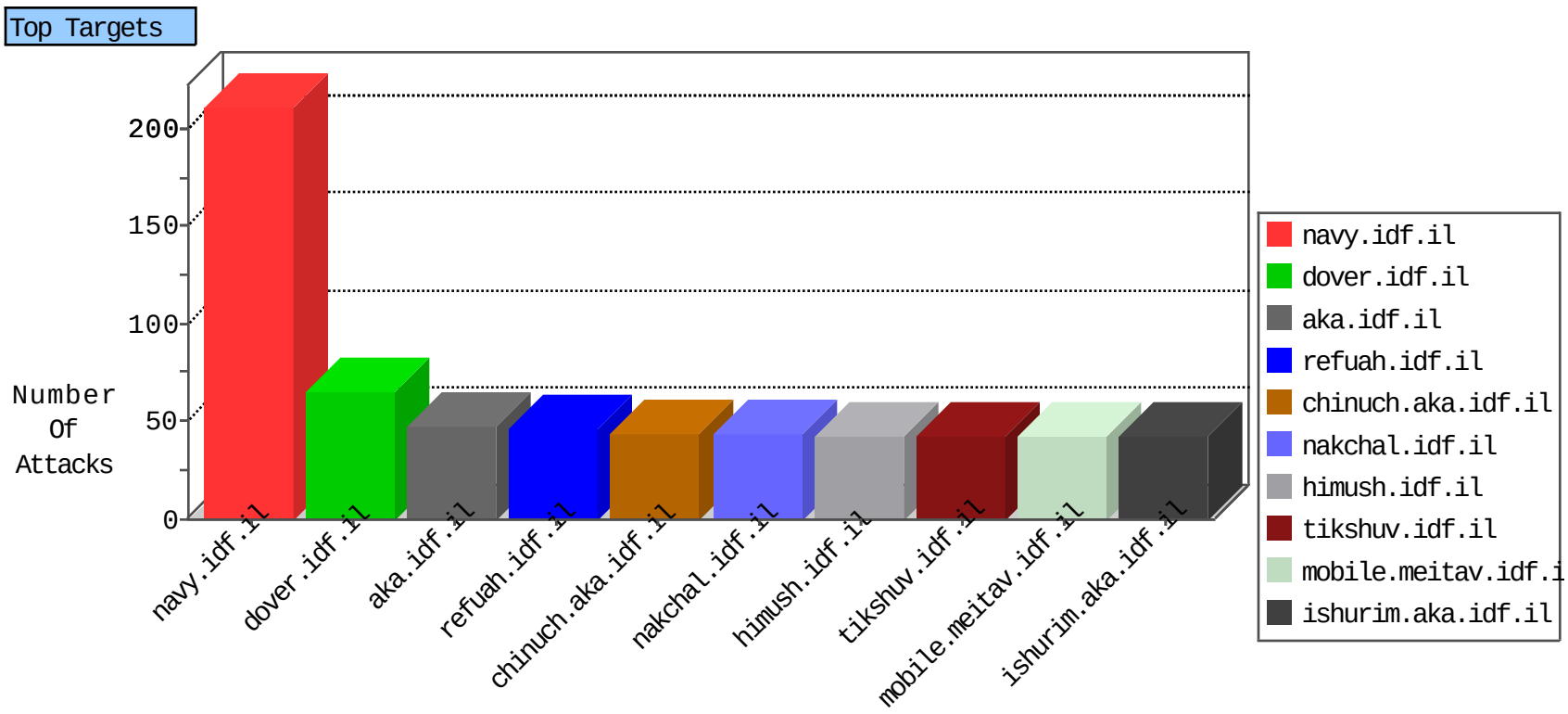
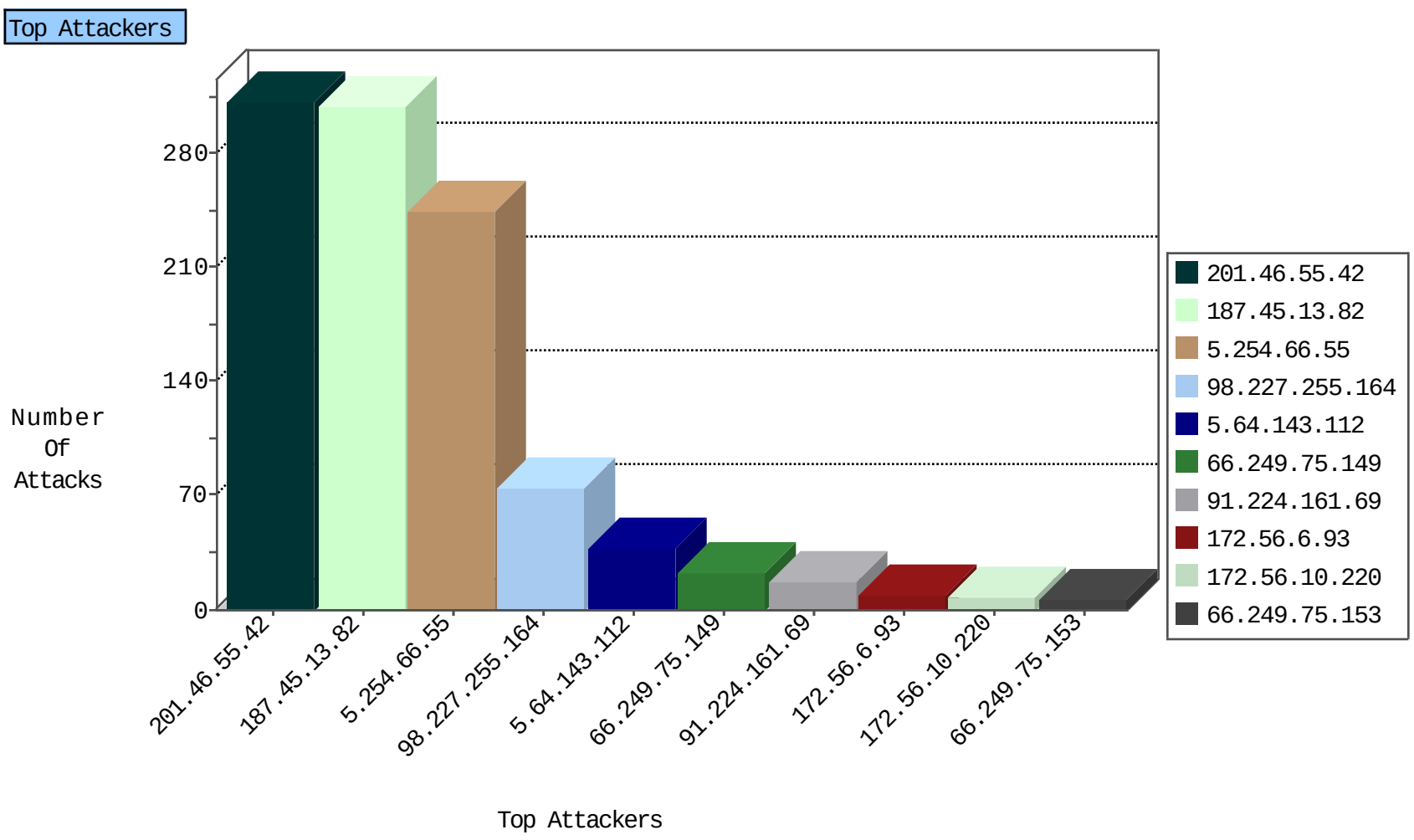
09-10-2016-06:04:02 to 09-10-2016-07:04:02

IDF Under Attack Daily Report





09-10-2016-06:04:02 to 09-10-2016-07:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.138.116	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
185.94.111.1	Russian Federation	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
185.94.111.1	Russian Federation	147.237.76.86	navy.idf.il	Black List	drop	1

09-10-2016-06:04:02 to 09-10-2016-07:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-10-2016-06:04:02 to 09-10-2016-07:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
91.224.161.69	147.237.76.42	Netherlands	refuah.idf.il	ET SCAN Potential SSH Scan	3
91.224.161.69	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN Potential SSH Scan	2
91.224.161.69	147.237.76.202	Netherlands	e.halag.idf.il	ET SCAN Potential SSH Scan	2
91.224.161.69	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN Potential SSH Scan	2
108.28.45.211	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
67.222.16.47	147.237.72.217	United States	e.idf.il	GPL SCAN superscan echo	1
93.158.203.147	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
45.33.116.208	147.237.0.35	United States	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.224.161.69	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN Potential SSH Scan	1
91.224.161.69	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN Potential SSH Scan	1
91.224.161.69	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
197.44.94.31	147.237.77.234	Egypt	halag.idf.il	ET SCAN NMAP -sS window 4096	1
195.88.208.193	147.237.76.147	Russian Federation	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
139.162.168.200	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.224.161.69	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
123.176.80.201	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
69.24.208.162	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
93.158.203.147	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1
46.172.71.251	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
23.92.20.154	147.237.76.30	United States	himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.224.161.69	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
91.224.161.69	147.237.76.86	Netherlands	navy.idf.il	ET SCAN Potential SSH Scan	1
197.44.94.31	147.237.77.234	Egypt	halag.idf.il	ET SCAN NMAP -sS window 1024	1
91.224.161.69	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
176.58.124.35	147.237.76.201	United Kingdom	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
91.224.161.69	147.237.0.34	Netherlands	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
123.176.80.201	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
72.69.113.91	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sS window 4096	1

09-10-2016-06:04:02 to 09-10-2016-07:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
66.249.75.149	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
98.227.255.164	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
98.227.255.164	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	16
98.227.255.164	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	16
187.45.13.82	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.42	Brazil	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.42	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.42	Brazil	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
187.45.13.82	Brazil	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.42	Brazil	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
187.45.13.82	Brazil	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.42	Brazil	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.42	Brazil	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
187.45.13.82	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.42	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
187.45.13.82	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.42	Brazil	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.42	Brazil	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
187.45.13.82	Brazil	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
201.46.55.42	Brazil	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
187.45.13.82	Brazil	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
187.45.13.82	Brazil	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
201.46.55.42	Brazil	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
187.45.13.82	Brazil	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
5.254.66.55	Romania	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
187.45.13.82	Brazil	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
201.46.55.42	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
187.45.13.82	Brazil	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
187.45.13.82	Brazil	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
201.46.55.42	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
187.45.13.82	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
187.45.13.82	Brazil	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
201.46.55.42	Brazil	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
5.254.66.55	Romania	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
201.46.55.42	Brazil	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
187.45.13.82	Brazil	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
187.45.13.82	Brazil	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
187.45.13.82	Brazil	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
5.254.66.55	Romania	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
187.45.13.82	Brazil	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
5.254.66.55	Romania	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
201.46.55.42	Brazil	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
187.45.13.82	Brazil	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
5.254.66.55	Romania	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
201.46.55.42	Brazil	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
187.45.13.82	Brazil	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
187.45.13.82	Brazil	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
98.227.255.164	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
201.46.55.42	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
201.46.55.42	Brazil	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13

09-10-2016-06:04:02 to 09-10-2016-07:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.123.93.127	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	2
68.180.228.240	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
157.55.39.20	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
66.249.66.174	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
157.55.39.109	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1392-en/cogat.asp	Block	1
66.249.66.233	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/)	Block	1
79.181.186.38	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush	Block	1
157.55.39.224	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.224	Block	1
66.249.75.149	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/894-he	Block	1
115.28.71.161	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.64.228	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/602-2265-he/patzar.aspx	Block	1
157.55.39.227	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
66.249.76.70	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/robots.txt	Block	1
115.28.71.161	China	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/wp-login.php	Block	1
66.249.65.156	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1482-he/atal.aspx	Block	1

09-10-2016-06:04:02 to 09-10-2016-07:04:02