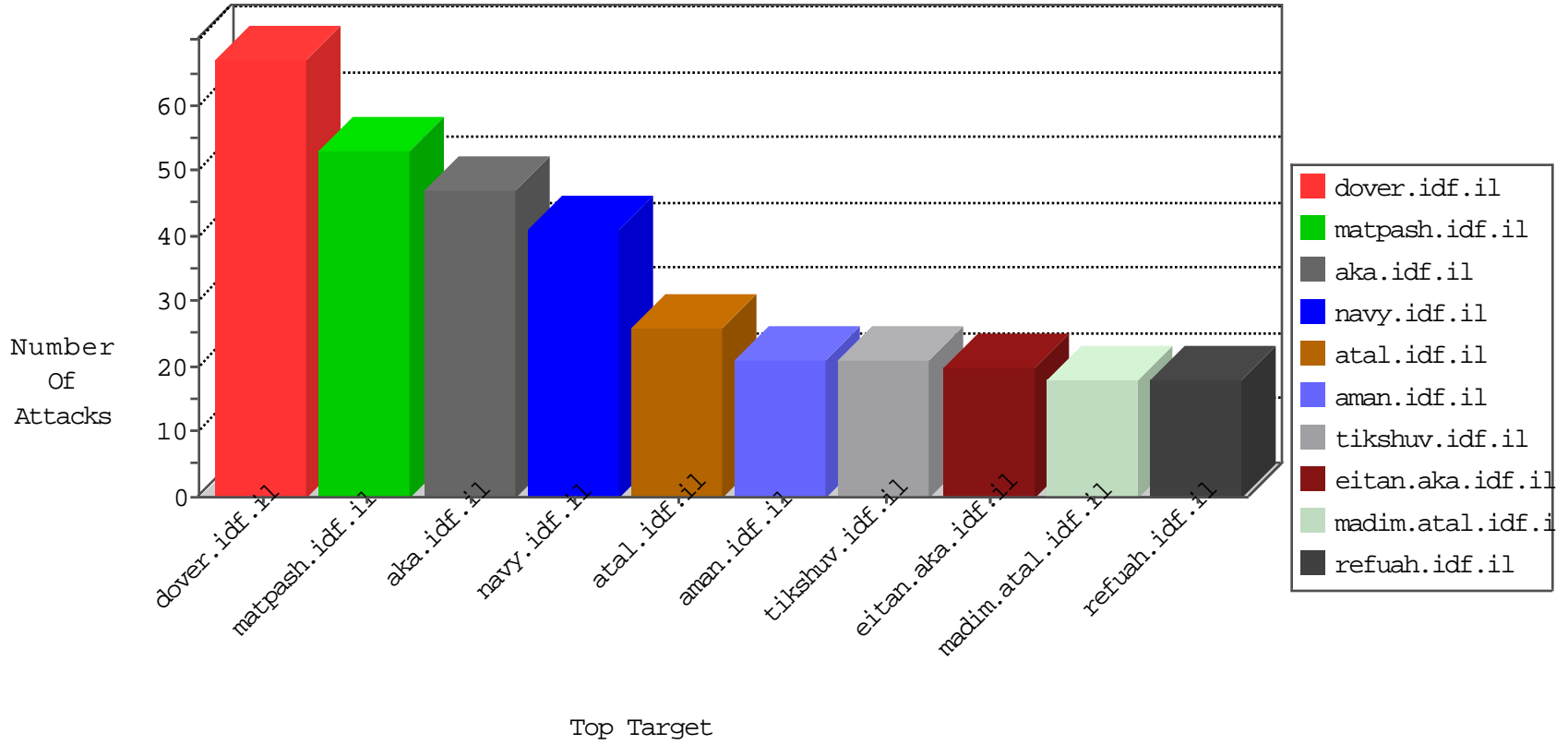


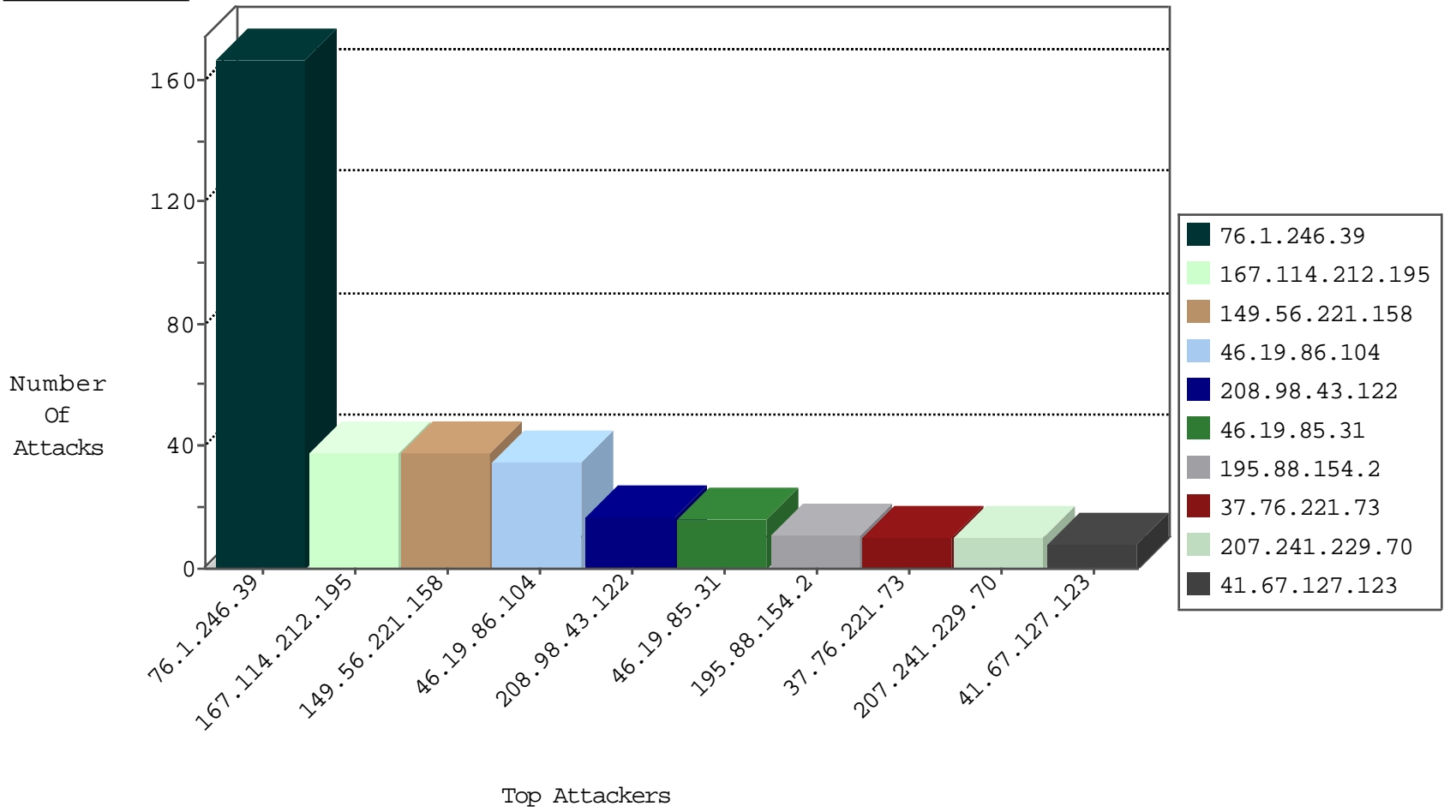
# IDF Under Attack Daily Report



Top Targets



Top Attackers



## Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.67.127.123	Egypt	147.237.77.216	dover.idf.il	HTTP-MISC-Acunetix-Url	dest-reset	4
218.93.206.21	China	147.237.76.44	e.refuah.idf.il	JLM_Under_Attack_Con_Top	drop	2

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.67.127.123	Egypt	147.237.77.216	dover.idf.i	10767: HTTP: Acunetix Security Scanner	Block	1
41.67.127.123	Egypt	147.237.77.216	dover.idf.i	13465: HTTP: Apache Roller OGNL Command Injection Vulnerability	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
80.246.133.197	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDoS attack	3
176.248.219.53	147.237.77.216	United Kingdom	dover.idf.il	Xenu Link Sleuth User Agent	2
46.120.122.219	147.237.77.170	Israel	maarachot.idf.il	Xenu Link Sleuth User Agent	2
52.74.147.121	147.237.77.235	Singapore	sviva.idf.il	ET SCAN NMAP -f -sS	1
193.201.225.138	147.237.77.205	Ukraine	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
23.91.75.231	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.67.13	147.237.77.212	United Kingdom	e.dover.idf.il	ET SCAN Potential SSH Scan	1
163.172.67.13	147.237.76.198	United Kingdom	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
163.172.67.13	147.237.8.46	United Kingdom	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
116.12.175.233	147.237.0.19	Singapore	madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
116.12.175.233	147.237.0.19	Singapore	madim.atal.idf.il	ET SCAN NMAP -f -sS	1
52.74.147.121	147.237.77.235	Singapore	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
208.67.1.220	147.237.76.197	United States	e.himush.idf.il	ET SCAN Potential SSH Scan	1
191.114.202.105	147.237.8.28	Chile	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
163.172.169.150	147.237.77.212	United Kingdom	e.dover.idf.il	ET SCAN Potential SSH Scan	1
163.172.67.13	147.237.77.61	United Kingdom	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
163.172.67.13	147.237.72.14	United Kingdom	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
163.172.67.13	147.237.8.24	United Kingdom	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
116.12.175.233	147.237.0.19	Singapore	madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
208.100.26.228	147.237.72.156	United States	aman.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
76.1.246.39	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
76.1.246.39	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
207.241.229.70	United States	147.237.77.216	dover.idf.il	Web Server Enforcement Violation	Web Servers Slow HTTP Denial of Service	reject	10
76.1.246.39	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
76.1.246.39	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
76.1.246.39	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
76.1.246.39	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
76.1.246.39	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
76.1.246.39	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
46.19.85.31	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
37.76.221.73	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
76.1.246.39	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.86.104	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
76.1.246.39	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
76.1.246.39	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
76.1.246.39	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
76.1.246.39	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
76.1.246.39	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.86.104	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
76.1.246.39	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
76.1.246.39	United States	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
76.1.246.39	United States	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.86.104	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
76.1.246.39	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.85.31	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.9	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
76.1.246.39	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
76.1.246.39	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
76.1.246.39	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
76.1.246.39	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
46.19.86.104	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
138.246.253.19	Germany	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
46.120.246.91	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
149.56.221.158	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
149.56.221.158	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
149.56.221.158	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
5.22.134.239	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
85.65.23.44	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.85.146	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
68.174.122.103	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
46.19.86.137	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.53.15.10	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.120.246.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	3
149.56.221.158	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
149.56.221.158	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.86.212	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.76.221.73	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	3
149.56.221.158	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
171.234.181.240	Vietnam	147.237.77.176	matpash.idf.il	Parameter Type Violation SortDir in www.cogat.idf.il/1038-en/cogat.aspx	Block	3
109.64.81.190	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
207.46.13.57	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
79.178.88.72	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 79.178.88.72	Block	1
66.249.69.83	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/eitan/pratim/pirteychayal/	Block	1
157.55.39.115	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
66.249.76.115	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-14594-he/dover.aspx	Block	1
41.67.127.123	Egypt	147.237.77.216	dover.idf.il	Malformed URL www.acunetix.wvs:443	Block	1
79.178.88.72	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/3/	Block	1
66.249.69.101	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/sip_storage/files/0/880.pdf	Block	1
68.180.229.39	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakchal.idf.il/1117-he/nakhal.aspx	Block	1
41.67.127.123	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/console/j_security_check	Block	1
66.249.69.119	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/forums/asp/showforum.asp	Block	1
176.248.219.53	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/	Block	1
77.138.154.87	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/atudalane.aspx	Block	1
46.19.86.137	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
119.129.52.86	China	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 119.129.52.86	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.76.75	Block	1
185.77.91.109	Turkey	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to 147.237.0.19/index.php	Block	1
78.46.42.235	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
66.249.66.239	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/pages/reports.aspx	Block	1
119.129.52.86	China	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1