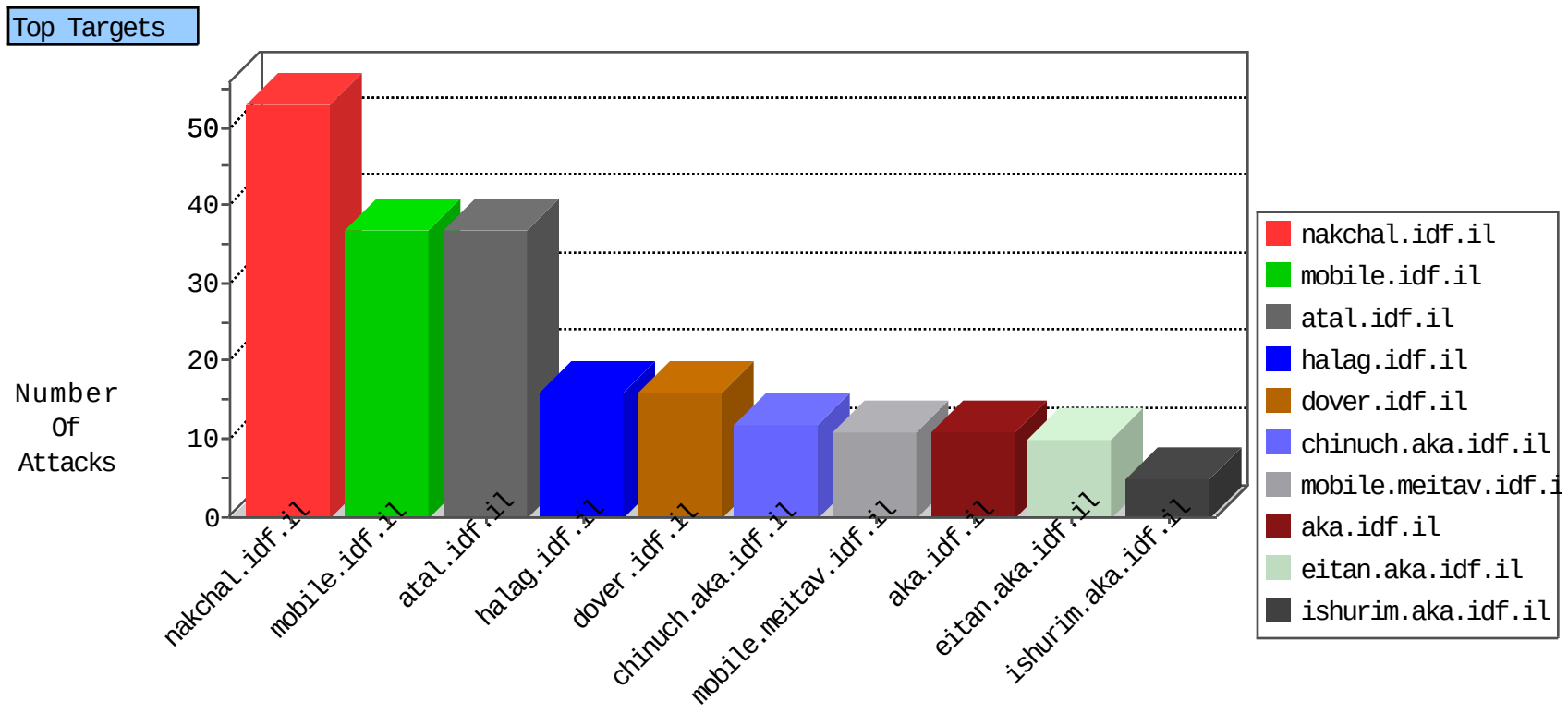
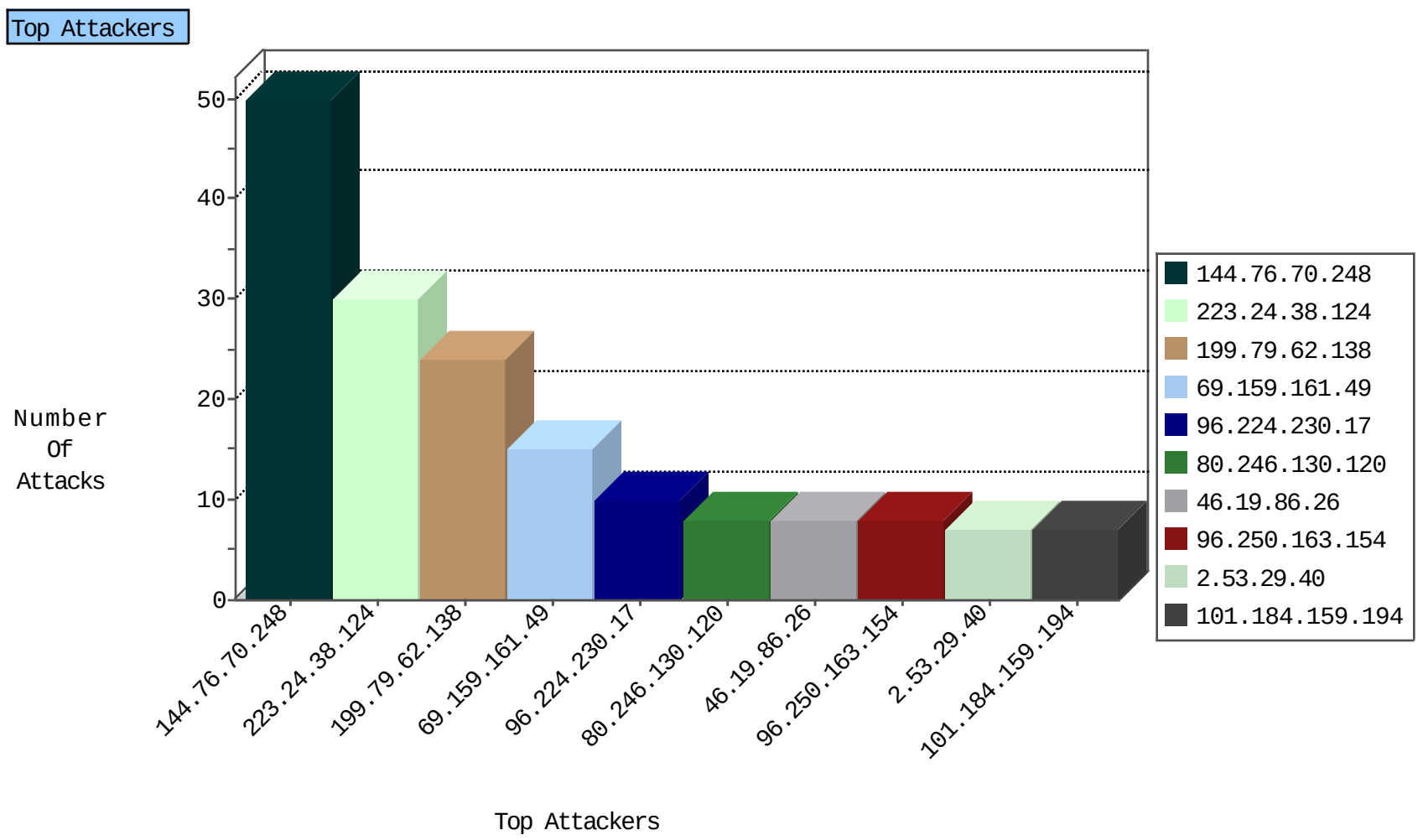
09-25-2016-05:04:00 to 09-25-2016-06:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-25-2016-05:04:00 to 09-25-2016-06:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
114.79.26.41	Indonesia	147.237.76.177	ncore.idf.il	Black List	drop	3
222.186.34.141	China	147.237.77.178	e.matpash.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
222.186.34.141	China	147.237.77.227	e.hamaz.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
120.70.17.51	China	147.237.76.30	himush.idf.il	Black List	drop	1

09-25-2016-05:04:00 to 09-25-2016-06:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
144.76.70.248	Germany	147.237.76.31	nakchal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	12
144.76.70.248	Germany	147.237.76.31	nakchal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
199.79.62.138	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
144.76.70.248	Germany	147.237.76.31	nakchal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2

09-25-2016-05:04:00 to 09-25-2016-06:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
144.76.70.248	147.237.76.31	Germany	nakchal.idf.il	SQL Injection - Select From	26
199.79.62.138	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	18
80.246.130.120	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
211.149.244.79	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
110.159.32.84	147.237.77.233	Malaysia	atal.idf.il	ET SCAN NMAP -sS window 4096	1
110.159.32.84	147.237.77.233	Malaysia	atal.idf.il	ET SCAN NMAP -f -sS	1
82.18.209.67	147.237.77.178	United Kingdom	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
58.220.2.5	147.237.8.45	China	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
46.183.223.228	147.237.0.15	Latvia	kosher-kravi.idf.i	ET SCAN Potential SSH Scan	1
139.162.187.89	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
110.159.32.84	147.237.77.233	Malaysia	atal.idf.il	ET SCAN NMAP -sS window 2048	1
88.249.106.23	147.237.0.15	Turkey	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
58.220.2.5	147.237.8.27	China	e.madim.atal.idf.i	ET SCAN NMAP -sS window 1024	1

09-25-2016-05:04:00 to 09-25-2016-06:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
223.24.38.124	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
69.159.161.49	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
96.224.230.17	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.62	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
69.159.161.49	Canada	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
96.250.163.154	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
101.184.159.194	Australia	147.237.76.39	mobile.meitav.idf.i	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
46.19.86.26	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
80.246.130.120	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
96.250.163.154	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
101.184.159.194	Australia	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
79.183.96.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.168	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.26	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
96.224.230.17	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
37.26.148.192	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence		alert	2
37.26.148.192	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence		monitor	2
37.26.148.192	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
172.58.145.162	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
91.185.190.172	Poland	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
192.0.113.146	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.82.47.54	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
46.19.85.59	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
184.105.139.72	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.86.26	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	1
46.19.85.59	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
184.105.139.111	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
216.218.240.235	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
119.81.248.53	Hong Kong	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
184.105.247.200	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
139.162.37.147	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
91.185.190.172	Poland	147.237.76.39	mobile.meitav.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.247.212	United States	147.237.77.179	e.mazi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-25-2016-05:04:00 to 09-25-2016-06:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.29.40	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	7
176.13.3.114	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	4
80.246.136.209	Israel	147.237.0.19	madim.atal.idf.i	Suspicious Response Code	Block	2
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
46.19.85.62	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
77.124.37.26	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
46.19.86.26	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
66.102.9.2	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
31.154.81.65	Israel	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2388.jpg	Block	1
31.154.81.65	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1

09-25-2016-05:04:00 to 09-25-2016-06:04:00