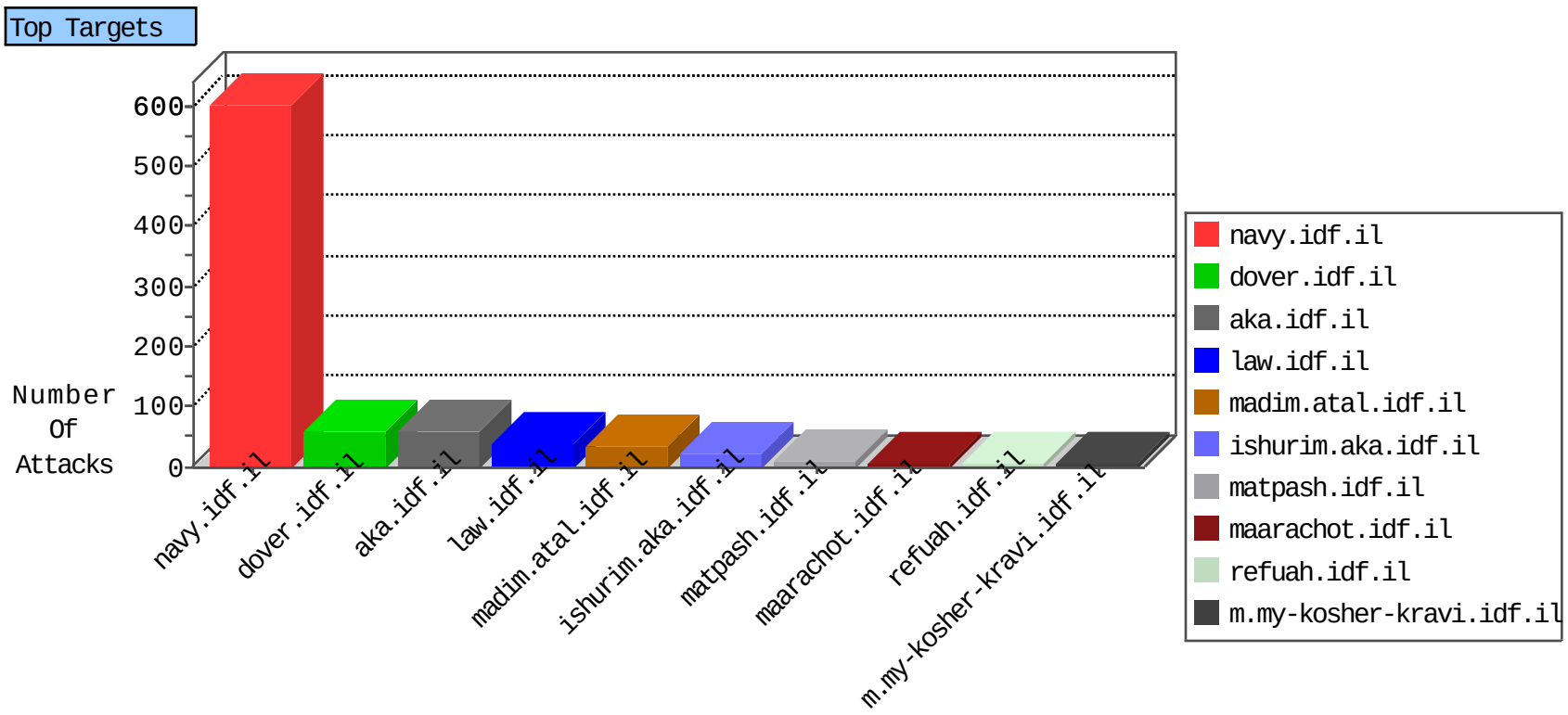
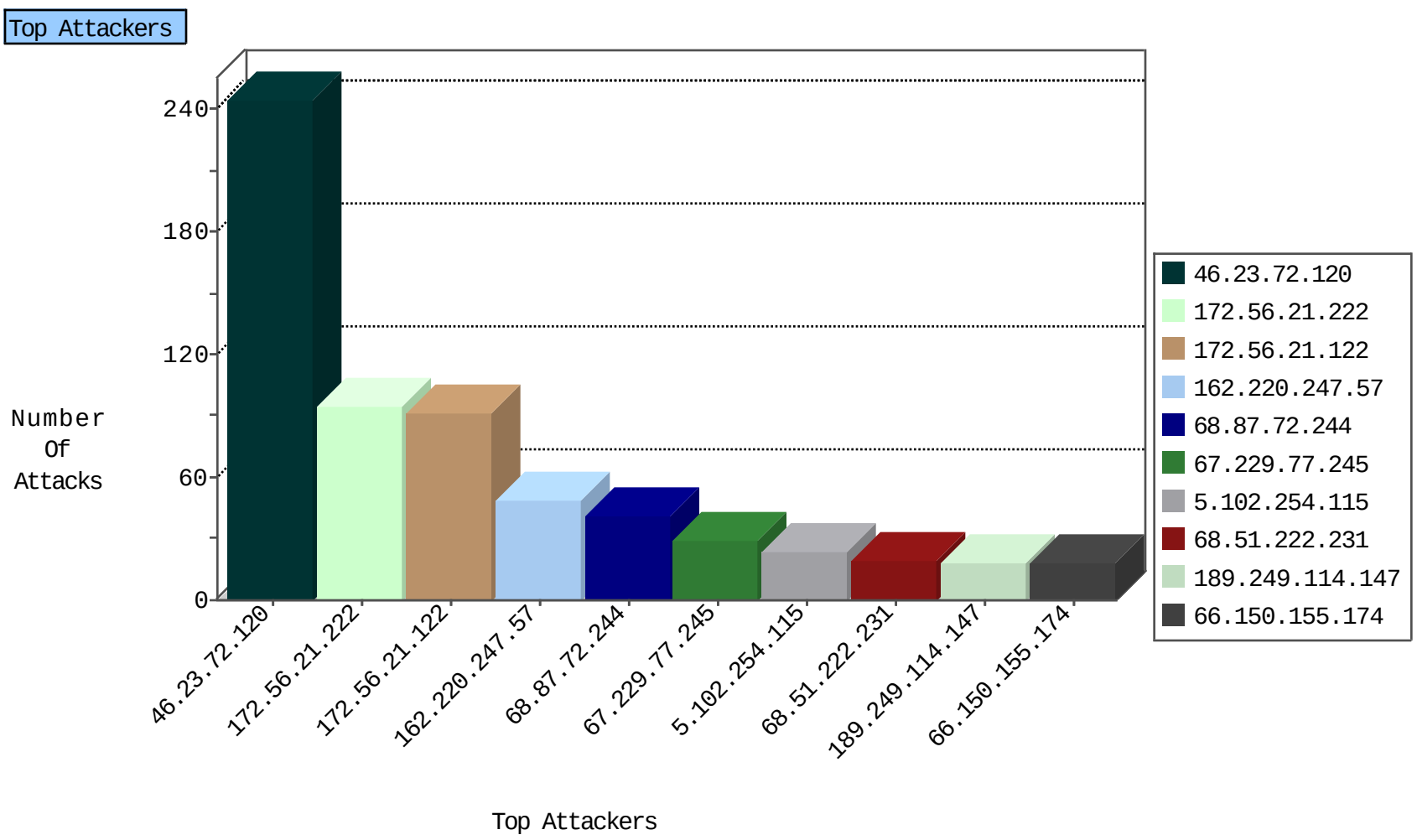
09-11-2016-06:04:06 to 09-11-2016-07:04:06

IDF Under Attack Daily Report





09-11-2016-06:04:06 to 09-11-2016-07:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	5
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	4
129.97.74.14	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
164.107.127.12	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
130.206.158.138	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.22.150.78	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
147.83.29.234	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.223.8.112	United States	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
194.29.178.13	Poland	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
134.117.226.180	Canada	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
129.22.150.78	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
119.57.253.157	China	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
134.117.226.180	Canada	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
129.32.84.160	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
193.1.13.12	Ireland	147.237.72.14	dover.idf.il(old)	network flood IPv4 ICMP	drop	1
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-11-2016-06:04:06 to 09-11-2016-07:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
97.74.215.165	United States	147.237.77.74	law.idf.i	5670: HTTP: SQL Injection (SELECT)	Block	6
158.85.253.245	United States	147.237.77.74	law.idf.i	5670: HTTP: SQL Injection (SELECT)	Block	6
199.87.254.195	United States	147.237.77.74	law.idf.i	34161: ICMP: Communication with Destination Host is Administratively Prohibited (Code 10)	Block	1

09-11-2016-06:04:06 to 09-11-2016-07:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
97.74.215.165	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
158.85.253.245	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
66.249.93.217	147.237.77.176	Europe	matpash.idf.il	ET SCAN NMAP -sA (2)	1
46.161.40.17	147.237.72.167	Russian Federation	ishurim.aka.idf.il	ET SCAN Potential SSH Scan	1
211.141.78.56	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
191.96.249.18	147.237.8.24	Chile	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
176.47.81.138	147.237.77.216	Saudi Arabia	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
104.128.144.131	147.237.8.27	Canada	e.madim.atal.idf.il	ET SCAN NMAP -sS window 2048	1
46.172.71.251	147.237.72.14	Ukraine	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
211.141.78.56	147.237.77.74	China	law.idf.il	ET SCAN NMAP -sS window 1024	1
178.220.165.231	147.237.77.74		law.idf.il	ET SCAN NMAP -sS window 1024	1
104.128.144.131	147.237.8.27	Canada	e.madim.atal.idf.il	ET SCAN NMAP -f -sS	1

09-11-2016-06:04:06 to 09-11-2016-07:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.23.72.120	Netherlands	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	189
46.23.72.120	Netherlands	147.237.76.86	navy.idf.il	SYN Attack		monitor	50
162.220.247.57	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	38
172.56.21.222	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
172.56.21.222	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	20
172.56.21.122	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	19
172.56.21.122	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	19
172.56.21.222	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	19
172.56.21.122	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	18
172.56.21.222	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
172.56.21.122	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	18
66.150.155.174	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
172.56.21.222	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	17
172.56.21.122	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
37.26.149.167	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	16
162.220.247.57	United States	147.237.76.86	navy.idf.il	SYN Attack		monitor	11
24.187.233.90	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
46.19.86.118	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
69.126.129.217	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
98.126.23.45	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.23.72.120	Netherlands	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
178.255.153.114	Switzerland	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
2.53.142.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
178.255.153.114	Switzerland	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
2.53.142.57	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
68.51.222.231	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	4
189.249.114.147	Mexico	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
199.203.179.99	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	4
68.51.222.231	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	4
189.249.114.147	Mexico	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
68.51.222.231	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
189.249.114.147	Mexico	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	4
68.51.222.231	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
178.255.153.114	Switzerland	147.237.76.86	navy.idf.il	SYN Attack		monitor	3
68.51.222.231	United States	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.253.196.253	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
189.249.114.147	Mexico	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	3
94.103.101.74	Switzerland	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
5.22.134.207	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
189.249.114.147	Mexico	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
91.214.170.63	Switzerland	147.237.76.86	navy.idf.il	SYN Attack		monitor	3
130.193.50.33	Russian Federation	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
68.87.72.244	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
37.142.80.88	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
68.87.72.244	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
68.87.72.244	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
68.87.72.244	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
68.87.72.244	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
68.87.72.244	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2

09-11-2016-06:04:06 to 09-11-2016-07:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.102.254.115	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
67.229.77.245	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 67.229.77.245	Block	17
67.229.77.245	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
91.244.149.159	Ukraine	147.237.77.176	matpash.idf.il	Parameter Type Violation lang in www.cogat.idf.il/1038-en/cogat.aspx	Block	4
185.32.179.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	2
84.95.208.20	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
66.249.66.177	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
5.22.134.207	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
139.162.13.205	Singapore	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Untraceable SSL Sessions from 139.162.13.205 (Protocol violation (SSL_CONN_CLIENT_HELLO))	None	1
84.108.51.177	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layoutdev.css	Block	1
87.69.248.129	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
188.120.154.8	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
67.229.77.245	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
91.244.149.159	Ukraine	147.237.77.176	matpash.idf.il	Parameter Type Violation SortDir in www.cogat.idf.il/1038-en/cogat.aspx	Block	1
46.19.86.137	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
204.79.180.95	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/miluim/templates/inner.asp	Block	1

09-11-2016-06:04:06 to 09-11-2016-07:04:06