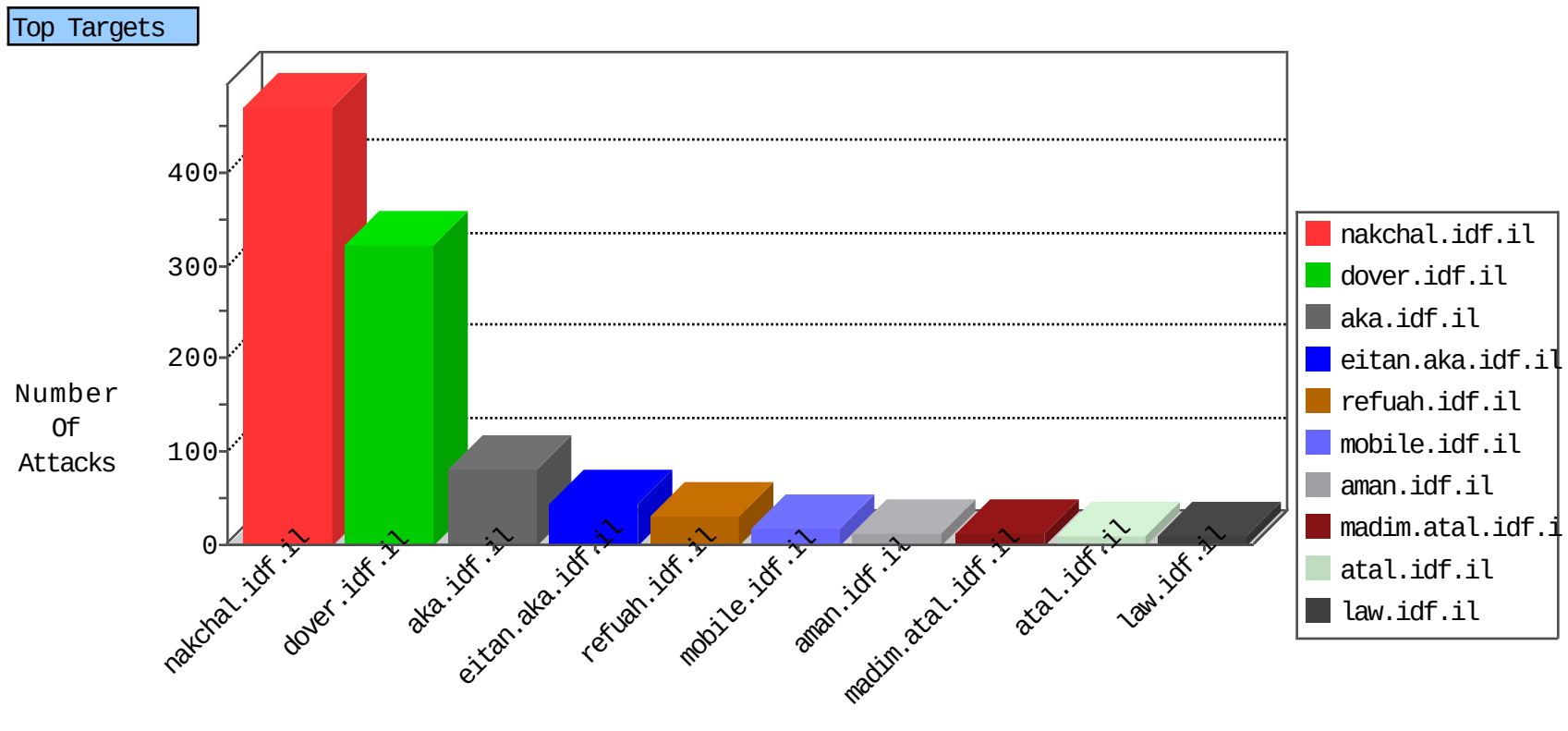
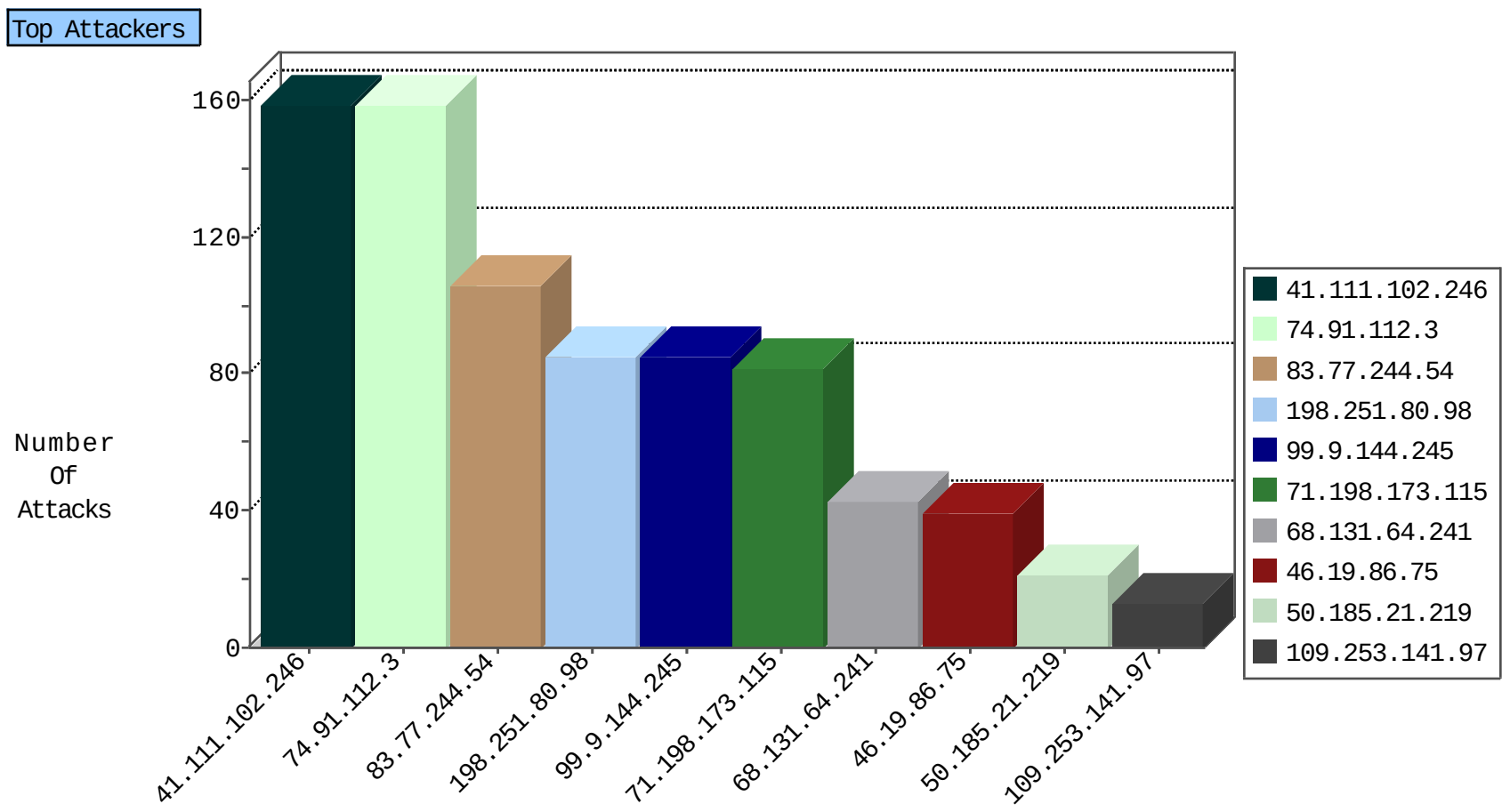
09-28-2016-00:04:03 to 09-28-2016-01:04:03

IDF Under Attack
Daily Report

Top Targets



Top Attackers



09-28-2016-00:04:03 to 09-28-2016-01:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.141.15	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
93.174.94.235	Netherlands	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
198.167.138.185	United States	147.237.76.199	e.nakchal.idf.il	Black List	drop	1
93.174.94.235	Netherlands	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1
93.174.94.235	Netherlands	147.237.76.202	e.halag.idf.il	Black List	drop	1

09-28-2016-00:04:03 to 09-28-2016-01:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

09-28-2016-00:04:03 to 09-28-2016-01:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
210.4.8.235	147.237.0.17	Philippines	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	2
188.212.249.187	147.237.8.46	Romania	e.chinuch.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	2
91.201.236.50	147.237.76.31	Ukraine	nakchal.idf.il	ET SCAN NMAP -f -sS	1
46.19.86.127	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
210.4.8.235	147.237.76.44	Philippines	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
210.4.8.235	147.237.72.156	Philippines	aman.idf.il	ET SCAN Potential SSH Scan	1
108.6.128.112	147.237.0.33	United States	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.50	147.237.76.31	Ukraine	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
89.139.152.222	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
210.4.8.235	147.237.76.86	Philippines	navy.idf.il	ET SCAN Potential SSH Scan	1
210.4.8.235	147.237.76.34	Philippines	yohalan.idf.il	ET SCAN Potential SSH Scan	1
210.4.8.235	147.237.0.35	Philippines	akaws.idf.il	ET SCAN Potential SSH Scan	1
210.4.8.235	147.237.0.16	Philippines	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
125.38.178.28	147.237.77.179	China	e.mazi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
91.201.236.50	147.237.76.31	Ukraine	nakchal.idf.il	ET SCAN NMAP -sS window 2048	1

09-28-2016-00:04:03 to 09-28-2016-01:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.111.102.246	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	91
71.198.173.115	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	42
71.198.173.115	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	40
74.91.112.3	United States	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	34
74.91.112.3	United States	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	32
74.91.112.3	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	32
68.131.64.241	United States	147.237.76.200	eitan.aka.idf..	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
74.91.112.3	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	31
74.91.112.3	United States	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	30
83.77.244.54	Switzerland	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	25
83.77.244.54	Switzerland	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	24
198.251.80.98	United States	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	22
198.251.80.98	United States	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	21
198.251.80.98	United States	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
83.77.244.54	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	20
83.77.244.54	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	20
99.9.144.245	United States	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
99.9.144.245	United States	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	19
99.9.144.245	United States	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	18
83.77.244.54	Switzerland	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
99.9.144.245	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
99.9.144.245	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	12
198.251.80.98	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
198.251.80.98	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	10
109.253.141.97	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
50.185.21.219	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
50.185.21.219	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.86.75	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.86.75	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.85.75	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
217.132.48.209	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.157	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.178.129.102	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.75	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
81.218.80.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.185.61.12	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.22	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
46.19.86.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
46.120.2.249	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
109.253.141.97	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
50.185.21.219	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
46.19.86.75	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
172.56.40.94	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
77.138.196.69	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
109.253.141.15	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
79.178.129.102	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3

09-28-2016-00:04:03 to 09-28-2016-01:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.111.102.246	Algeria	147.237.77.216	dover.idf.il	Post Request - Missing Content Type from 41.111.102.246	Block	64
80.246.138.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
66.249.66.177	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	3
84.108.40.8	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	2
68.131.64.241	United States	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 68.131.64.241	Block	2
84.111.227.174	Israel	147.237.72.156	aman.idf.il	Suspicious Response Code	Block	2
176.13.4.116	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
79.152.244.165	Spain	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/giyus/	Block	1
66.249.69.127	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9236-he/refuah.aspx	Block	1
185.120.126.17	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1412-he/atal.aspx	Block	1
84.111.227.174	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1
68.131.64.241	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/1105-en/contactus.aspx	Block	1
176.13.224.7	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.179.6.251	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/pirsumeymofet.aspx	None	1
66.249.76.31	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/apple-app-site-association	Block	1
217.132.48.209	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.253.141.15	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 109.253.141.15 (Open Mode)	None	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1398-en/dover.aspx	Block	1
52.221.247.102	Singapore	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/web-console/serverinfo.jsp	Block	1
176.65.25.214	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
66.249.79.16	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/apple-app-site-association	Block	1
109.253.141.15	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
75.82.191.213	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
179.218.168.217	Brazil	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	1
166.137.118.61	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/ishurim/main/	Block	1
77.138.237.37	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.66.180	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
180.76.15.6	China	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/994-8944-he/refuah.aspx	Block	1
68.131.64.241	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized Method HEAD for eitan.aka.idf.il/1094-8149-en/eitan.aspx	None	1

09-28-2016-00:04:03 to 09-28-2016-01:04:03