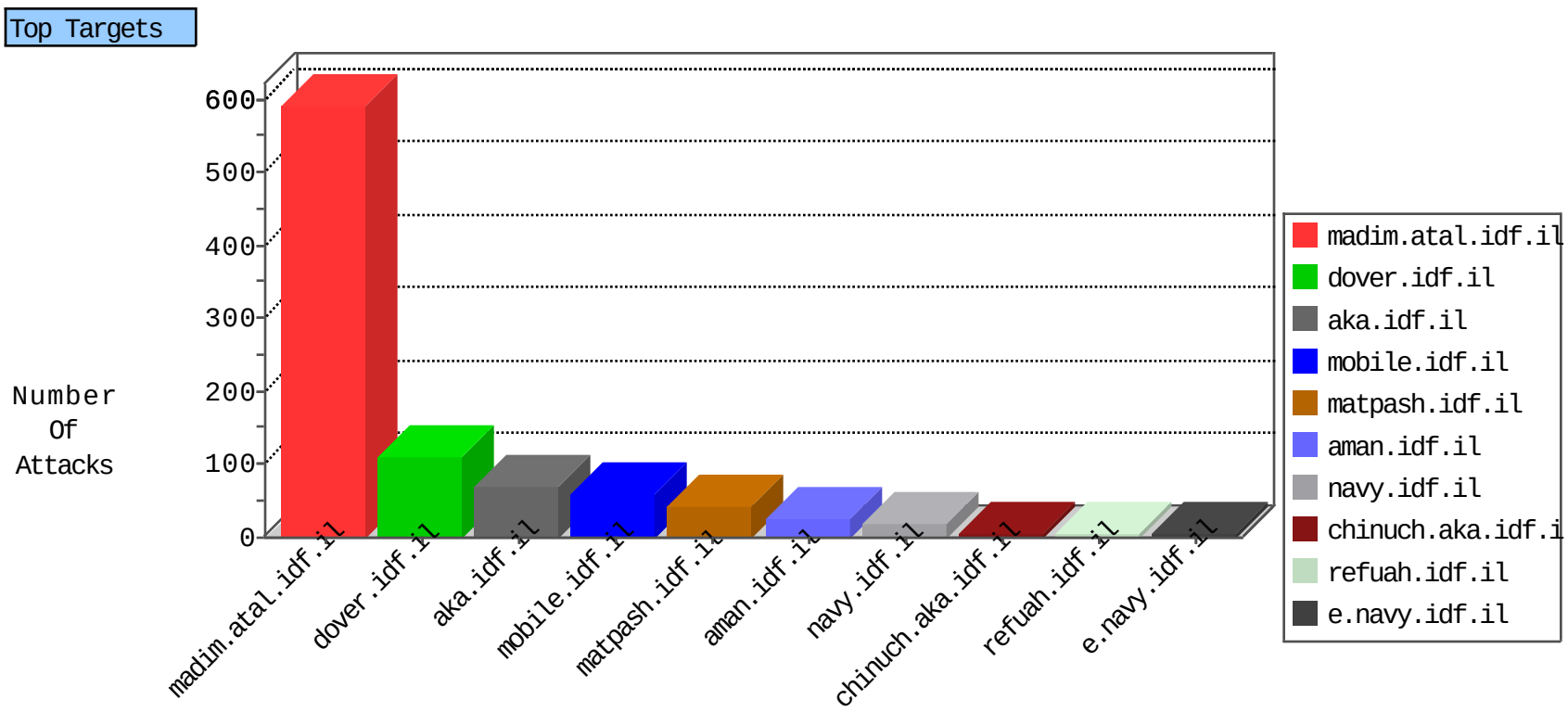
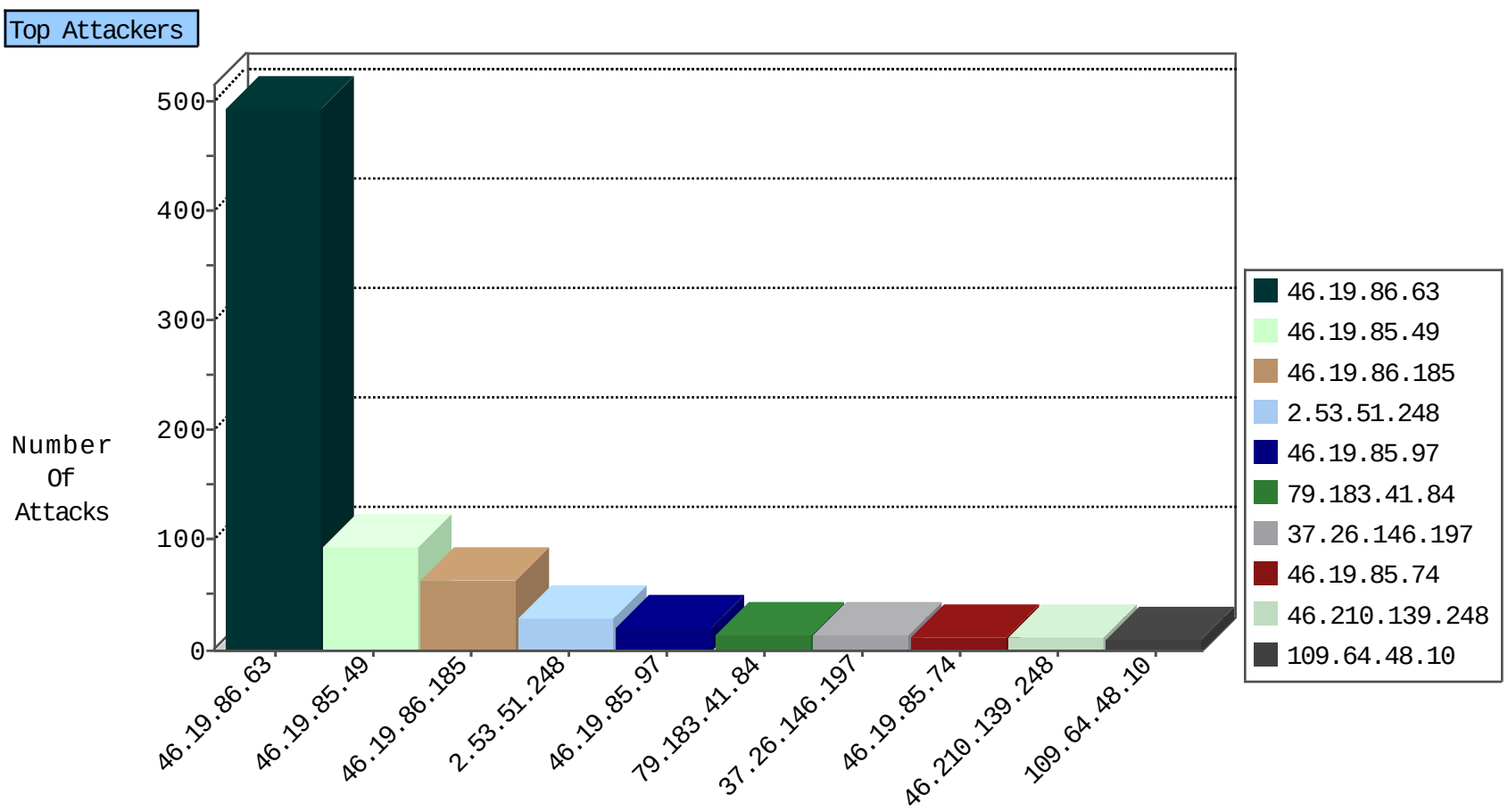
09-24-2016-13:04:01 to 09-24-2016-14:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-24-2016-13:04:01 to 09-24-2016-14:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
63.141.242.195	United States	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
94.177.177.128	Romania	147.237.76.198	e.yohalan.idf.il	Black List	drop	1
69.30.226.219	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	1
94.177.177.128	Romania	147.237.76.197	e.himush.idf.il	Black List	drop	1

09-24-2016-13:04:01 to 09-24-2016-14:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
162.210.196.97	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2

09-24-2016-13:04:01 to 09-24-2016-14:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
179.43.141.221	147.237.77.233	Switzerland	atal.idf.il	ET SCAN Potential SSH Scan	1
107.191.55.97	147.237.77.243	United States	mobile.idf.il	ET SCAN Potential SSH Scan	1
107.191.55.97	147.237.8.14	United States	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
91.201.236.158	147.237.77.121	Ukraine	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
91.201.236.155	147.237.76.30	Ukraine	himush.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.155	147.237.76.30	Ukraine	himush.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
123.31.34.244	147.237.77.61	Vietnam	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
107.191.55.97	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.77.121	Ukraine	e.navy.idf.il	ET SCAN NMAP -sS window 3072	1
91.201.236.158	147.237.77.121	Ukraine	e.navy.idf.il	ET SCAN NMAP -f -sS	1
91.201.236.155	147.237.76.30	Ukraine	himush.idf.il	ET SCAN NMAP -sS window 3072	1
46.183.223.228	147.237.76.38	Latvia	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1

09-24-2016-13:04:01 to 09-24-2016-14:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.53.51.248	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
37.26.146.197	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.97	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
46.19.85.97	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.74	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
109.64.48.10	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	9
46.19.86.128	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
77.99.147.20	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
46.19.86.185	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
46.19.86.185	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
79.183.41.84	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.185	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
46.210.139.248	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.185	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.183.41.84	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.185	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.210.139.248	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.86.185	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.96.191	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.185	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
85.65.134.217	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	5
46.117.43.167	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.86.185	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
84.52.98.134	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
210.162.15.11	Japan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.185	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.185	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.185.232.151	Jordan	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.185	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.86.185	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
87.70.37.150	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.185	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.118	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.185	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
213.57.169.167	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	3
46.19.86.50	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
77.139.175.83	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
109.253.199.90	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.74	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
37.26.147.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		alert	2
182.77.93.179	India	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
79.183.41.84	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
37.123.98.138	Turkey	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.19.86.50	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
79.177.8.133	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
37.26.147.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	2
46.19.86.22	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
192.116.128.90	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
37.123.98.138	Turkey	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	2

09-24-2016-13:04:01 to 09-24-2016-14:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.63	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	494
46.19.85.49	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	94
84.94.167.80	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	2
37.26.146.197	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.249.66.72	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/eitan/listpage/	Block	1
2.53.183.210	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
68.180.230.216	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1072-he/nakhal.aspx	Block	1
84.109.118.62	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
77.138.23.163	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
46.116.109.89	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
216.244.66.236	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/site/unselecatble.aspx	Block	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_text.asp	Block	1
40.77.167.17	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
77.139.49.68	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
54.225.80.243	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/miluim/about.aspx	Block	1
66.249.75.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-21533-ar/dover.aspx	Block	1
79.183.36.248	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/recruitlane.aspx	Block	1
66.102.9.3	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.76.113	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
46.19.85.119	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1

09-24-2016-13:04:01 to 09-24-2016-14:04:01