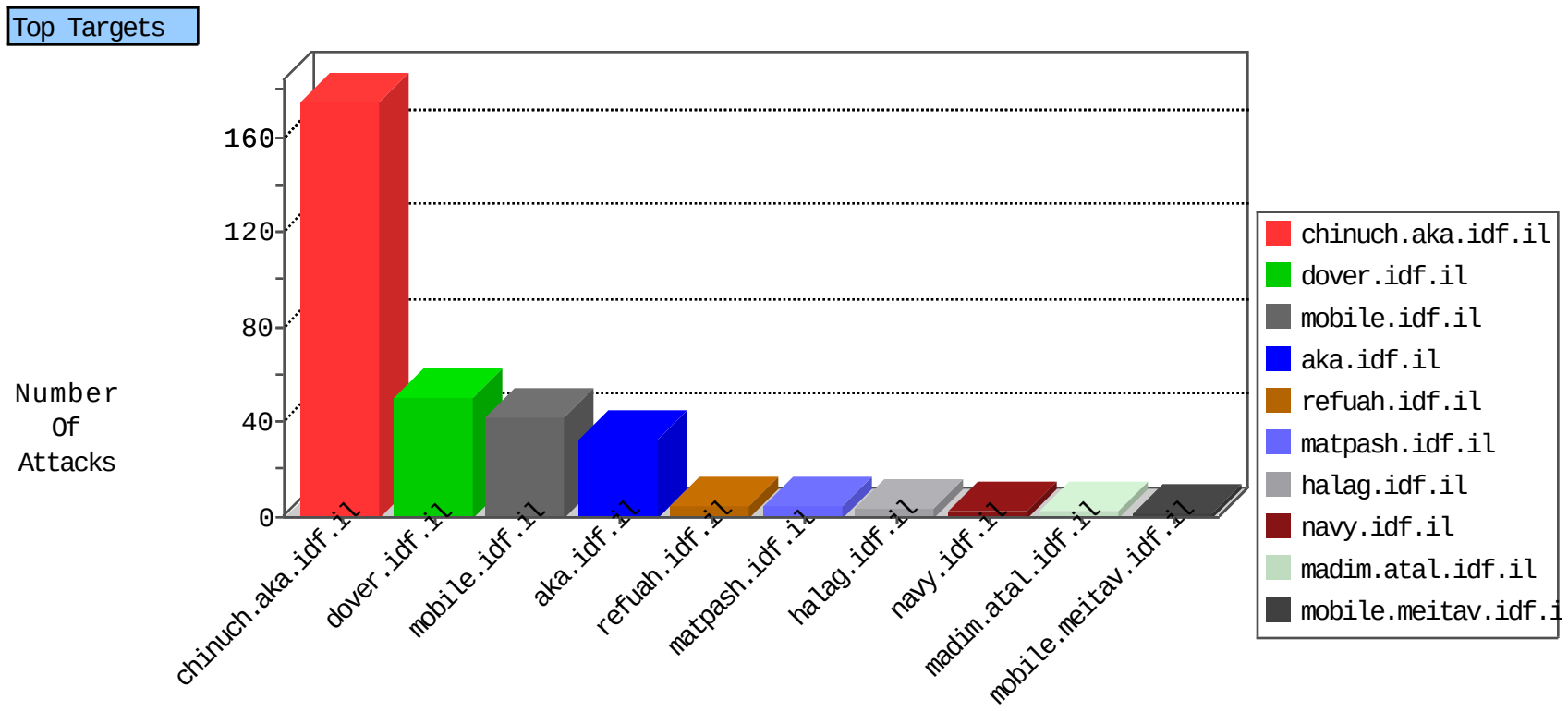
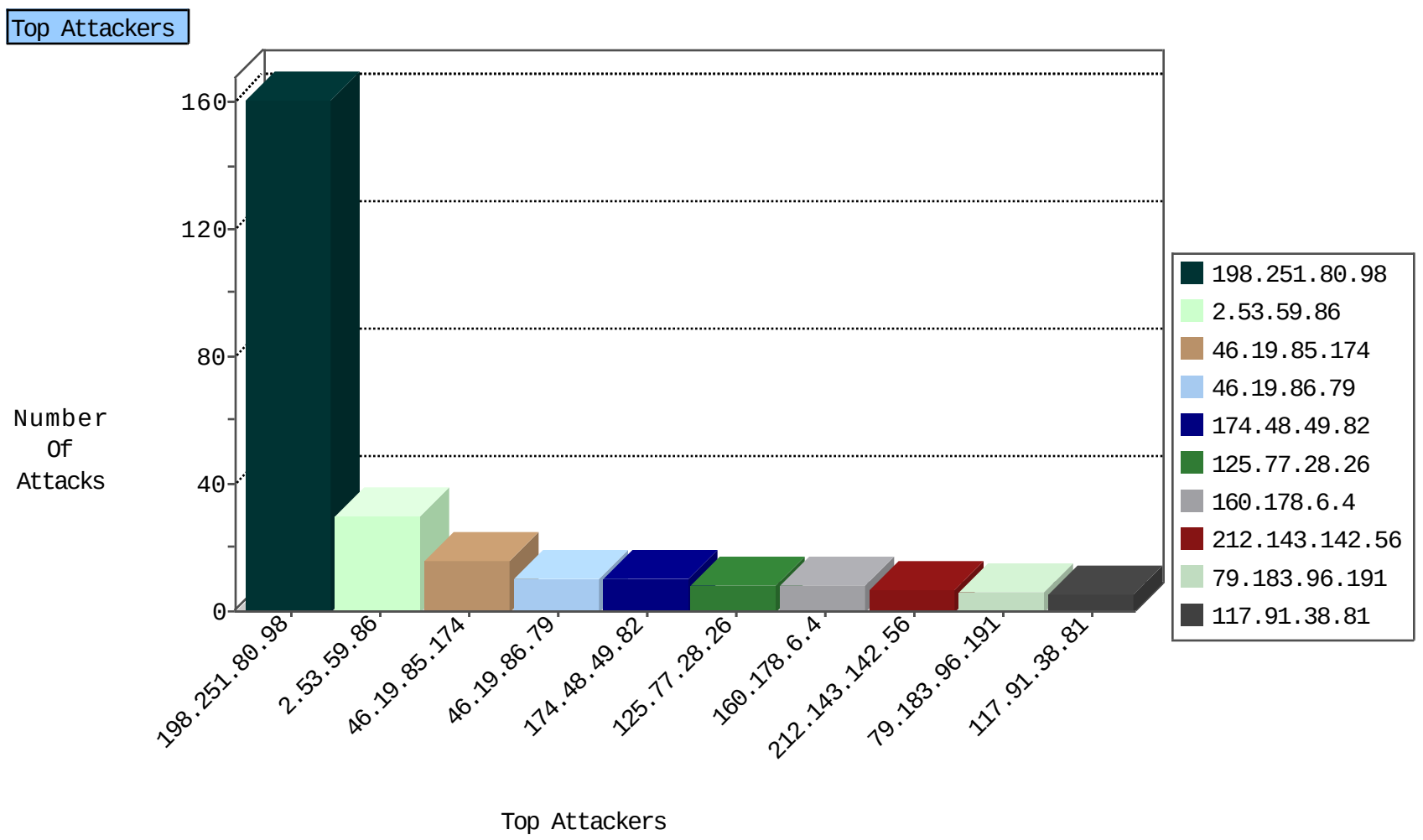
09-24-2016-01:07:43 to 09-24-2016-02:07:43

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-24-2016-01:07:43 to 09-24-2016-02:07:43

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
63.141.242.198	United States	147.237.76.30	himush.idf.il	block-sp-traf1	forward	2
69.30.227.220	United States	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
198.204.224.238	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
104.238.146.105	United States	147.237.76.42	refuah.idf.il	Black List	drop	1
173.244.198.5	United States	147.237.76.42	refuah.idf.il	Black List	drop	1
63.141.231.196	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
104.238.146.105	United States	147.237.76.34	yohalan.idf.il	Black List	drop	1
63.141.231.198	United States	147.237.0.19	madim.atal.idf.il	block-sp-traf1	forward	1
104.238.146.105	United States	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1

09-24-2016-01:07:43 to 09-24-2016-02:07:43

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.254.97.218	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
199.58.86.209	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	1

09-24-2016-01:07:43 to 09-24-2016-02:07:43

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
210.212.207.80	147.237.77.19	India	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
85.190.159.134	147.237.77.176	Germany	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
58.220.2.5	147.237.77.61	China	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
31.24.228.20	147.237.0.15	United Kingdom	kosher-kravi.idf.i	ET SCAN NMAP -sS window 1024	1
211.149.244.79	147.237.72.14	China	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
125.84.155.3	147.237.76.196	China	e.sviva.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
58.220.2.5	147.237.77.205	China	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
46.183.223.228	147.237.8.28	Latvia	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1

09-24-2016-01:07:43 to 09-24-2016-02:07:43

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	47
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	40
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	38
2.53.59.86	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	21
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	14
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.174	Israel	147.237.77.216	dover.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
46.19.85.174	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
174.48.49.82	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	3
2.53.4.252	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
46.19.86.79	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
79.180.89.45	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.79	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	3
46.19.86.79	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.181.166.23	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
174.48.49.82	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	3
50.184.163.91	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
37.26.149.184	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.174	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
174.48.49.82	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
176.13.247.127	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
174.48.49.82	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
46.244.67.116	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
117.91.38.81	China	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	2
46.19.86.79	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
5.29.122.16	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
125.77.28.26	China	147.237.0.33	idf.il	drop		drop	1
95.93.229.55	Portugal	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
198.29.33.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
125.77.28.26	China	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
117.91.38.81	China	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
46.19.86.79	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
24.5.113.220	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
125.77.28.26	China	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
109.65.47.21	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
71.6.158.166	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
198.29.33.103	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
46.19.85.174	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
125.77.28.26	China	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
117.91.38.81	China	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
95.93.225.128	Portugal	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
46.19.86.79	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
176.13.226.35	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
125.77.28.26	China	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
109.65.87.224	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
77.138.104.88	France	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
117.91.38.81	China	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
95.93.225.128	Portugal	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	1
46.19.85.164	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1

09-24-2016-01:07:43 to 09-24-2016-02:07:43

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
160.178.6.4	Morocco	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 160.178.6.4	Block	4
66.249.69.228	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.228	Block	4
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	3
160.178.6.4	Morocco	147.237.77.216	dover.idf.il	Multiple Admin Blocking from 160.178.6.4	Block	2
77.139.159.97	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/drushim	Block	1
66.249.75.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-23074-ar/dover.aspx	Block	1
66.249.64.41	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/.well-known/assetlinks.json	Block	1
71.6.158.166	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/robots.txt	Block	1
85.74.97.34	Greece	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/2/4912.png	Block	1
66.249.75.38	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	1
66.249.64.116	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/usefulinformation/idkonim/pages/31012011yezu.aspx	Block	1
160.178.6.4	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/wp-login	Block	1
74.6.53.161	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/test/wp-admin/	Block	1
66.249.69.228	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	1
46.19.85.174	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
157.55.39.73	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.76.61	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/.well-known/assetlinks.json	Block	1
66.249.64.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/.well-known/apple-app-site-association	Block	1
217.69.133.85	Russian Federation	147.237.77.176	matpash.idf.il	Illegal Byte Code Character in URL /sip_storage/files/8/3688.pdf#012	Block	1
75.63.29.234	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/sip_storage/files/2/4912.png	Block	1
66.249.73.171	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/mobile/	Block	1
46.210.149.43	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	1
160.178.6.4	Morocco	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
66.249.76.62	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/apple-app-site-association	Block	1
66.249.66.72	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/templates/shared/usercontrols/navmenu/undefined	Block	1
77.138.99.170	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/rights/asp/info.asp	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/4/2294.jpg	Block	1
65.92.13.203	Canada	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
66.249.76.77	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/apple-app-site-association	Block	1

09-24-2016-01:07:43 to 09-24-2016-02:07:43