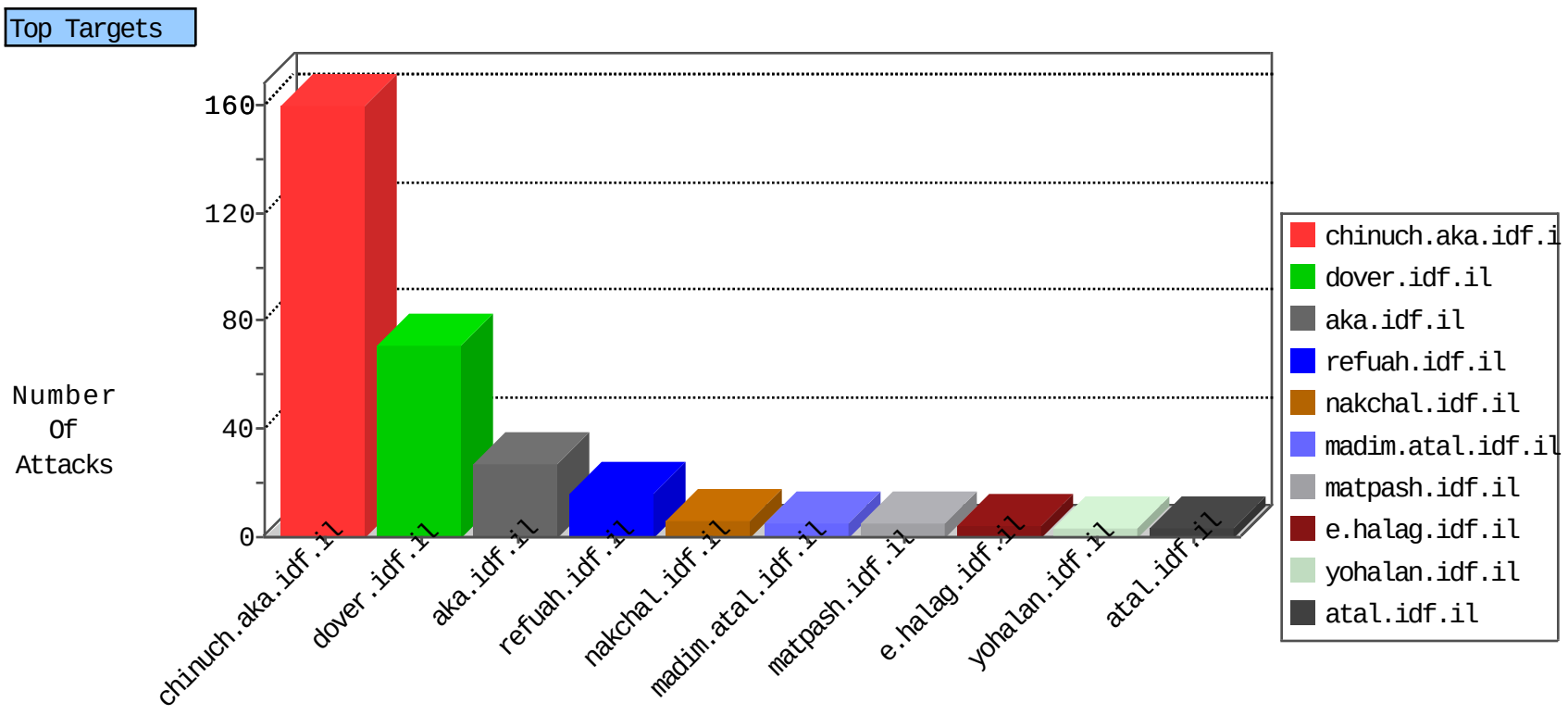
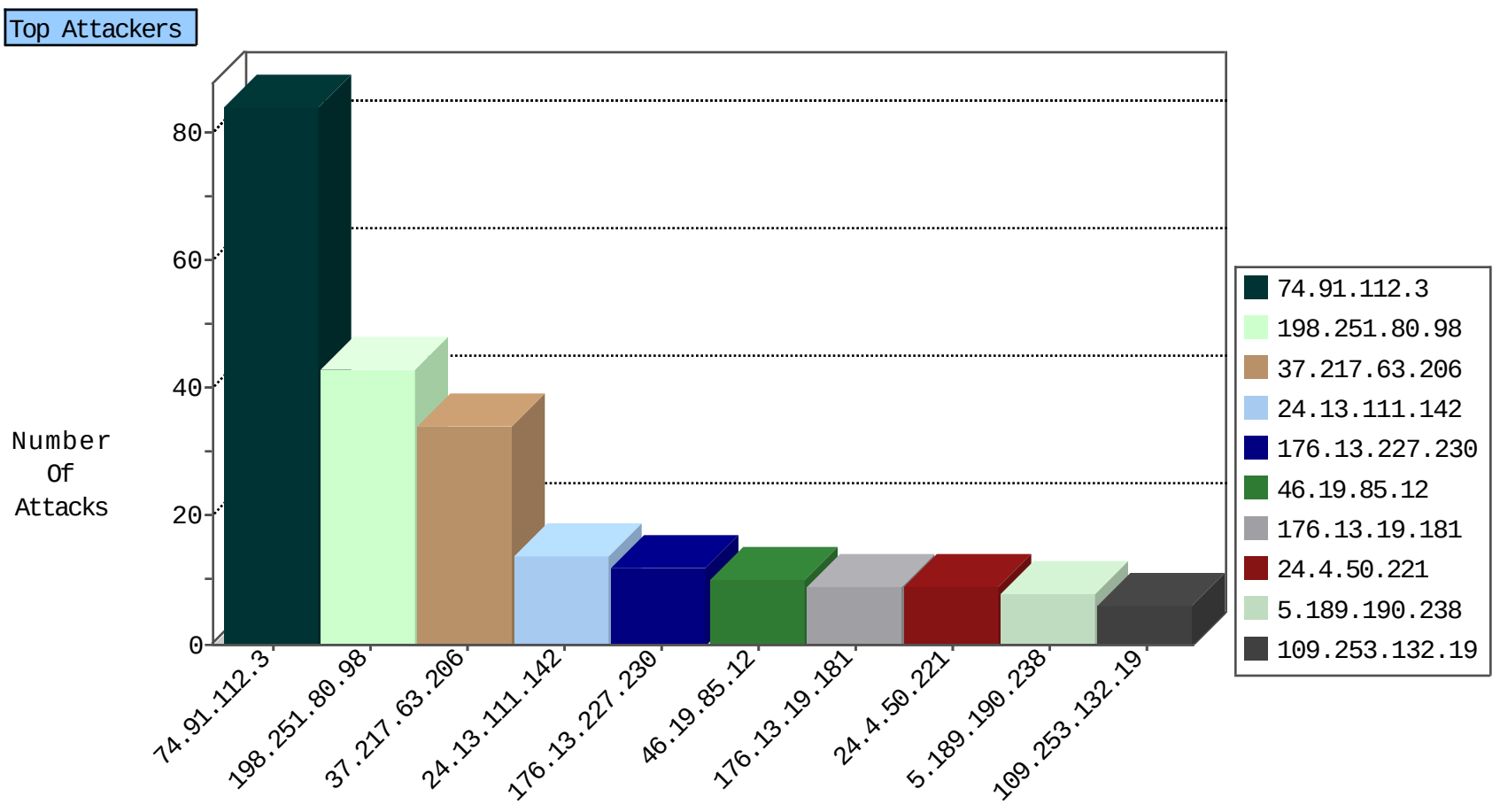
09-27-2016-03:04:08 to 09-27-2016-04:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-27-2016-03:04:08 to 09-27-2016-04:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
23.251.32.243	United States	147.237.76.201	e.atal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
89.248.172.16	Netherlands	147.237.76.38	e.e.meitav.idf.il	Black List	drop	1
104.238.144.29	United States	147.237.76.200	eitan.aka.idf.il	Black List	drop	1
208.67.1.248	United States	147.237.76.196	e.sviva.idf.il	Black List	drop	1
45.32.197.166	Netherlands	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1

09-27-2016-03:04:08 to 09-27-2016-04:04:08

Top Attackers In IPS

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

09-27-2016-03:04:08 to 09-27-2016-04:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
121.32.129.130	147.237.76.30	China	himush.idf.il	GPL SCAN nmap TCP	2
125.65.82.44	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.64.160	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
58.218.200.137	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
46.183.223.228	147.237.0.16	Latvia	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
45.63.28.148	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
198.252.110.108	147.237.77.216	United States	dover.idf.il	GPL SCAN superscan echo	1
2.50.129.104	147.237.77.212	United Arab Emirates	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
198.252.110.108	147.237.77.74	United States	law.idf.il	GPL SCAN superscan echo	1
2.50.129.104	147.237.77.212	United Arab Emirates	e.dover.idf.il	ET SCAN NMAP -f -sS	1
163.172.129.15	147.237.77.233	United Kingdom	atal.idf.il	ET SCAN NMAP -sS window 1024	1
149.255.108.192	147.237.76.39	United Kingdom	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
46.161.40.17	147.237.76.176	Russian Federation	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
45.63.28.148	147.237.76.31	United States	nakchal.idf.il	ET SCAN NMAP -f -sS	1
198.252.110.108	147.237.77.170	United States	maarachot.idf.il	GPL SCAN superscan echo	1
2.50.129.104	147.237.77.212	United Arab Emirates	e.dover.idf.il	ET SCAN NMAP -sS window 2048	1
185.129.148.230	147.237.76.200	Latvia	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
161.106.88.6	147.237.76.31	France	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1

09-27-2016-03:04:08 to 09-27-2016-04:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
37.217.63.206	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	34
74.91.112.3	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
74.91.112.3	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	18
74.91.112.3	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	17
74.91.112.3	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
74.91.112.3	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	13
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	11
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	10
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
176.13.19.181	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
109.253.132.19	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.12	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.12	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
186.176.14.67	Costa Rica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
176.13.227.230	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
176.13.227.230	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
176.13.227.230	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
24.13.111.142	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	3
176.13.19.181	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
24.13.111.142	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	3
24.13.111.142	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
84.108.40.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
24.13.111.142	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
24.4.50.221	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	2
46.19.85.144	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
24.4.50.221	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	2
62.210.90.118	France	147.237.77.216	dover.idf.il	drop	SAM rule	drop	2
89.139.214.200	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
24.4.50.221	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
84.108.40.147	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
24.13.111.142	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	2
24.4.50.221	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
186.90.105.127	Venezuela	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
191.218.212.53	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
169.229.3.91	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.169	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.189.190.238	Germany	147.237.76.34	yohalan.idf.il	drop		drop	1
85.64.205.157	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
186.90.105.127	Venezuela	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	1
74.82.47.33	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
149.56.121.185	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
5.189.190.238	Germany	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
139.162.37.147	United States	147.237.72.167	ishurim.aka.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
184.105.139.80	United States	147.237.0.35	akaws.idf.il	drop		drop	1
169.229.3.91	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.169	United States	147.237.77.61	e.cogat.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-27-2016-03:04:08 to 09-27-2016-04:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
157.55.39.46	United States	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to madim.atal.idf.il/robots.txt	Block	4
169.229.3.91	United States	147.237.76.86	navy.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.75.4	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 66.249.75.4	Block	1
72.53.134.34	Canada	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
177.16.54.151	Brazil	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/portalmiluim/templates/home.asp	Block	1
66.249.75.12	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9698-he/refuah.aspx	Block	1
66.249.69.228	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
186.176.14.67	Costa Rica	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.75.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
66.102.9.5	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
157.55.39.104	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
66.249.69.232	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_img.asp	Block	1
66.249.76.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
66.249.66.235	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.66.235	Block	1
157.55.39.160	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
66.249.73.190	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/iturim/asp/displayallsoldiers.asp	Block	1
68.180.231.60	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-ar/cogat.aspx	Block	1
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	1

09-27-2016-03:04:08 to 09-27-2016-04:04:08