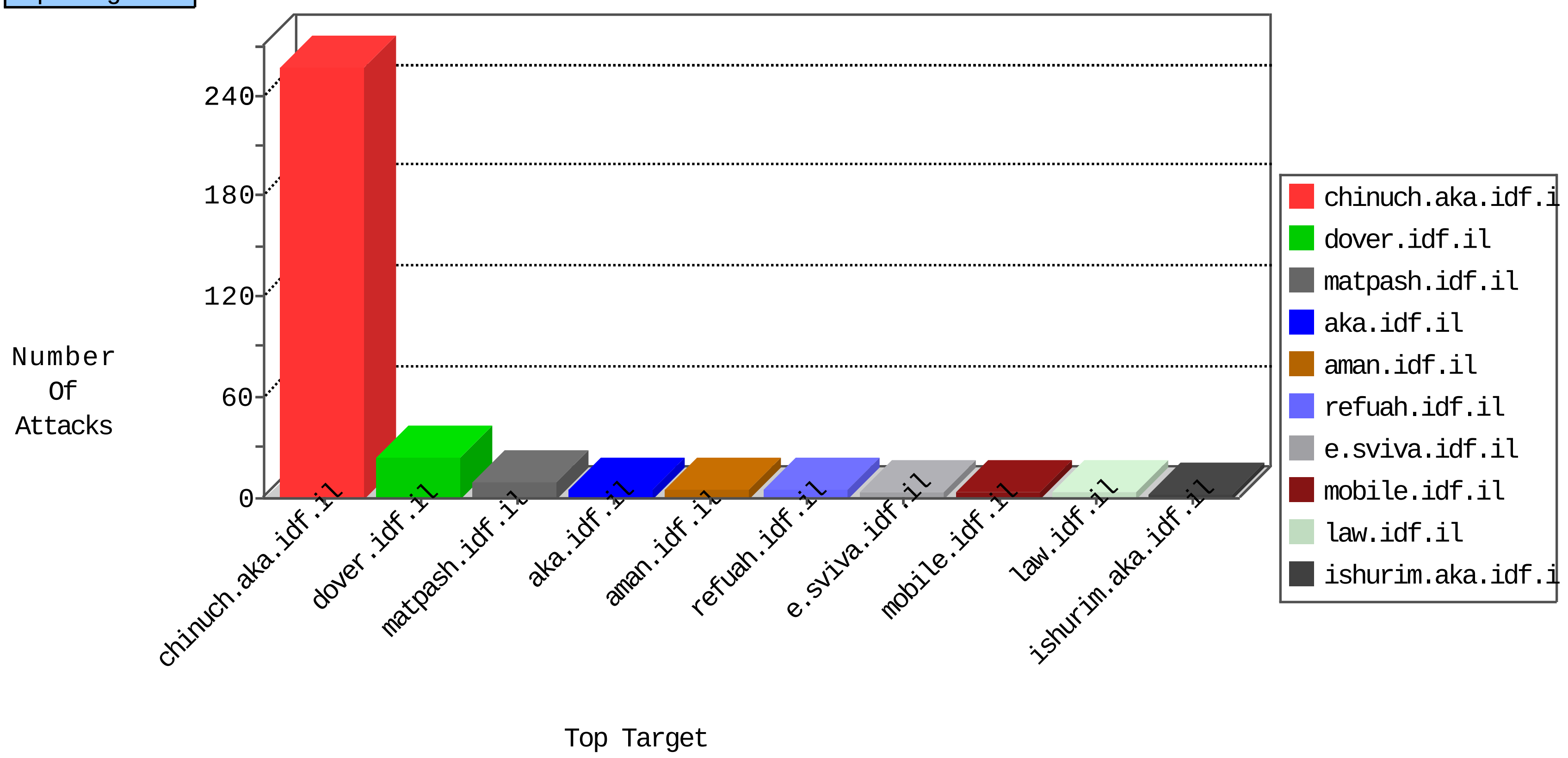
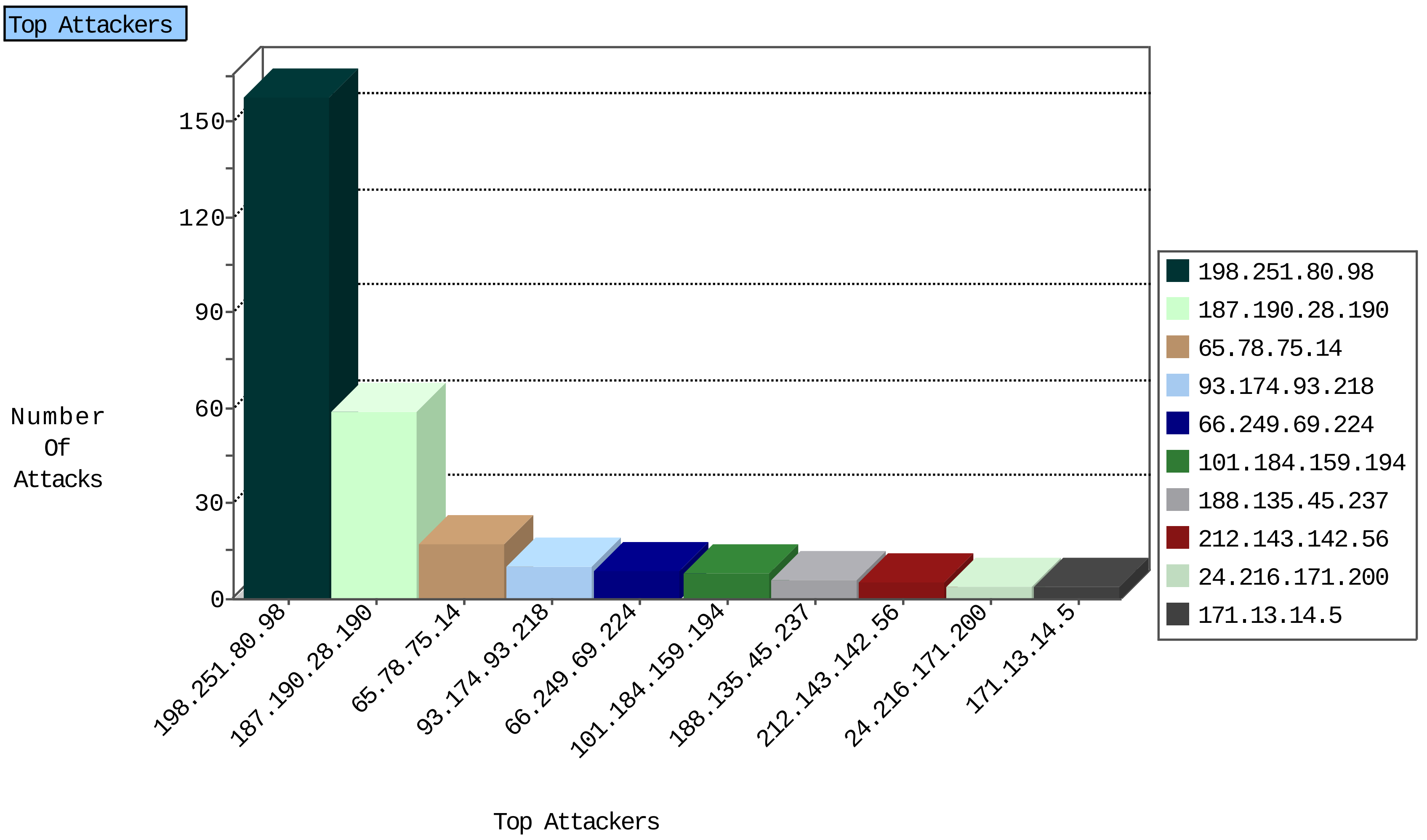
09-24-2016-05:04:09 to 09-24-2016-06:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



09-24-2016-05:04:09 to 09-24-2016-06:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
179.99.200.39	Brazil	147.237.76.42	refuah.idf.il	block-sp-traf1	forward	2
93.174.93.218	Netherlands	147.237.77.176	matpash.idf.il	block-sp-traf1	forward	2
134.147.203.115	Germany	147.237.76.196	e.sviva.idf.il	Black List	drop	2
52.53.222.9	United States	147.237.76.147	chinuch.aka.idf.il	Black List	drop	1
61.147.247.161	China	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
185.128.40.162	Switzerland	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1

09-24-2016-05:04:09 to 09-24-2016-06:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.135.45.237	Oman	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2

09-24-2016-05:04:09 to 09-24-2016-06:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
188.135.45.237	147.237.77.216	Oman	dover.idf.il	SQL Injection - Select From	3
179.43.141.221	147.237.76.39	Switzerland	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
113.240.250.154	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
113.240.250.154	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 1024	1
31.220.29.229	147.237.77.74	Italy	law.idf.il	ET SCAN NMAP -sS window 3072	1
194.60.242.6	147.237.77.212	Ukraine	e.dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
185.153.198.10	147.237.76.31		nakchal.idf.il	ET SCAN Potential SSH Scan	1
179.43.141.221	147.237.76.44	Switzerland	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
179.43.141.221	147.237.8.50	Switzerland	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
113.240.250.154	147.237.76.176	China	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
46.183.223.228	147.237.0.16	Latvia	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
31.220.29.229	147.237.77.74	Italy	law.idf.il	ET SCAN NMAP -sS window 1024	1
179.43.141.221	147.237.77.61	Switzerland	e.cogat.idf.il	ET SCAN Potential SSH Scan	1

09-24-2016-05:04:09 to 09-24-2016-06:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
187.190.28.190	Mexico	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	59
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	36
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	36
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	35
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	29
198.251.80.98	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	22
65.78.75.14	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	17
101.184.159.194	Australia	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
24.216.171.200	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
65.94.242.63	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
109.253.203.1	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
99.195.50.107	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
93.174.93.218	Netherlands	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Response out of state	monitor	2
171.13.14.5	China	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
67.166.152.219	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
184.105.247.220	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
141.212.122.62	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
68.198.10.40	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
179.99.200.39	Brazil	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
139.162.37.147	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.82.47.60	United States	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
216.52.148.178	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	1
37.26.149.218	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
157.55.39.113	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
74.82.47.9	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.139.74	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.50	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
77.139.204.175	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
216.52.148.178	United States	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	1
198.199.89.155	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
171.13.14.5	China	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
104.200.151.11	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
74.82.47.41	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
184.105.139.102	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.51	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
216.218.206.76	United States	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.82.47.45	United States	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
184.105.247.212	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.61	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
93.174.93.218	Netherlands	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
218.22.211.69	China	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
171.13.14.5	China	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
125.77.28.26	China	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
74.82.47.45	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
216.52.148.178	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1

09-24-2016-05:04:09 to 09-24-2016-06:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.69.224	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.224	Block	9
93.174.93.218	Netherlands	147.237.77.176	matpash.idf.il	Multiple NULL Character in Method from 93.174.93.218	Block	3
157.55.39.113	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/robots.txt	Block	1
66.249.69.232	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_img.asp	Block	1
180.76.15.162	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/clientscripts/jquery/' + url + '	Block	1
93.174.93.218	Netherlands	147.237.77.176	matpash.idf.il	Multiple Illegal Byte Code Character in Method from 93.174.93.218	Block	1
188.135.45.237	Oman	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/post	Block	1
204.79.180.88	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim/main/	Block	1
66.249.66.6	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/mobile/	Block	1
93.174.93.218	Netherlands	147.237.77.176	matpash.idf.il	NULL Character in Method	Block	1

09-24-2016-05:04:09 to 09-24-2016-06:04:09