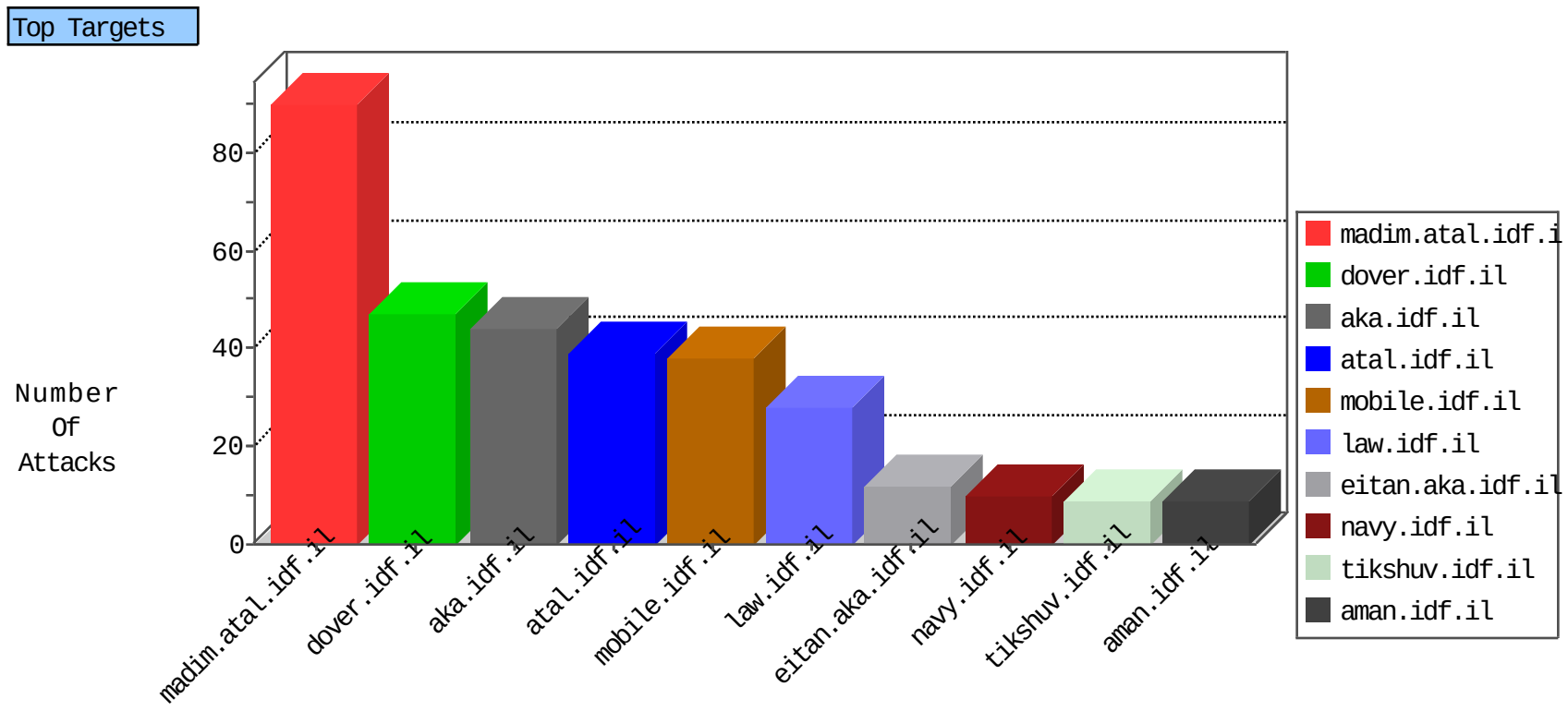
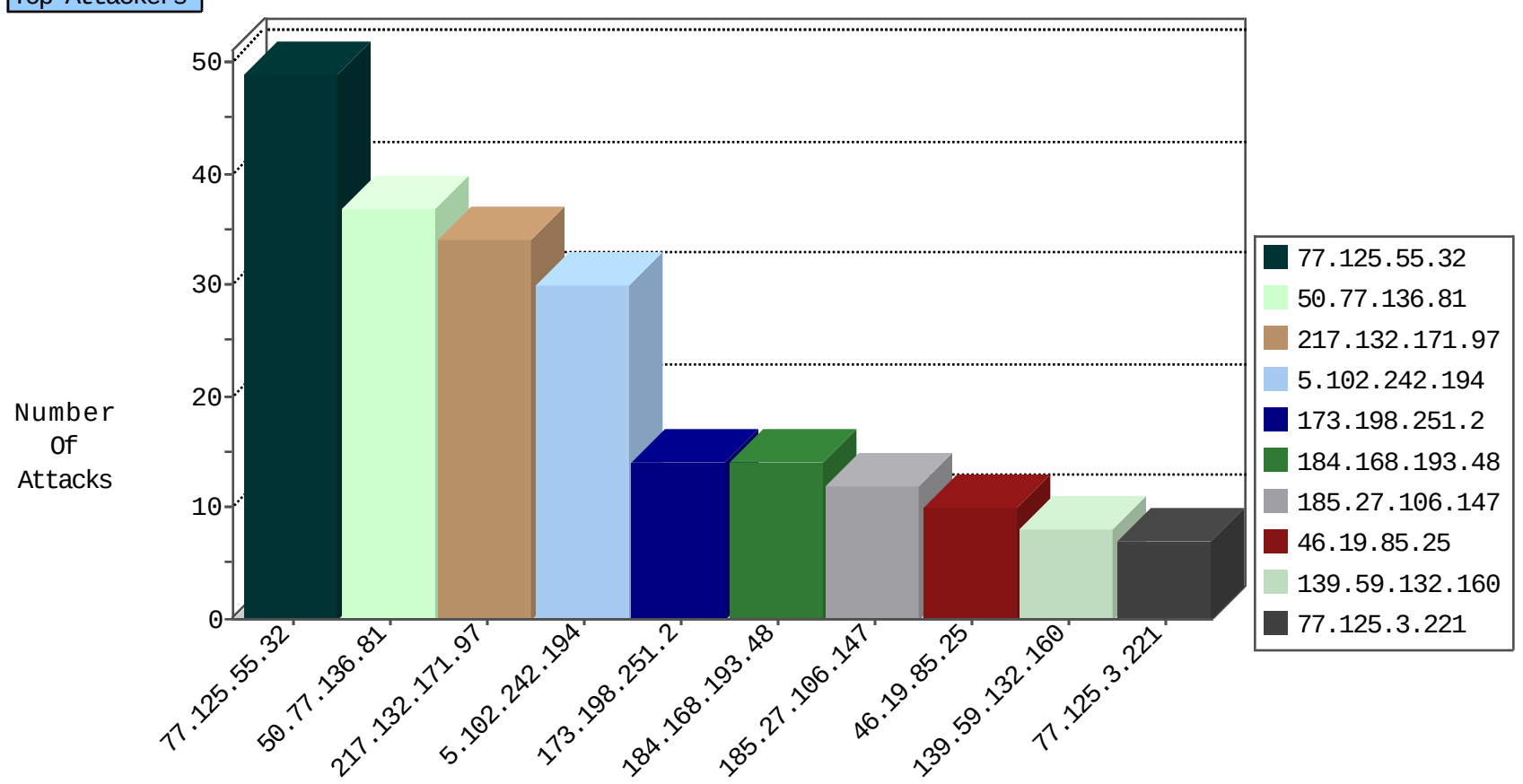
09-23-2016-00:04:00 to 09-23-2016-01:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



Top Attackers

09-23-2016-00:04:00 to 09-23-2016-01:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
85.64.168.182	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
185.128.40.162	Switzerland	147.237.76.38	e.e.meitav.idf.i	Black List	drop	1

09-23-2016-00:04:00 to 09-23-2016-01:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
50.77.136.81	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.77.136.81	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	6
173.198.251.2	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
184.168.193.48	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
50.77.136.81	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	6

09-23-2016-00:04:00 to 09-23-2016-01:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
50.77.136.81	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	19
173.198.251.2	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
184.168.193.48	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	8
223.100.131.151	147.237.76.30	China	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
40.121.139.43	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
208.80.155.255	147.237.77.216	United States	dover.idf.il	ET POLICY Incoming Basic Auth Base64 HTTP Password detected unencrypted	1
163.172.169.150	147.237.8.28	United Kingdom	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
64.137.168.128	147.237.0.16	Canada	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
46.161.40.17	147.237.0.33	Russian Federation	idf.il	ET SCAN NMAP -sS window 1024	1
40.121.139.43	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
211.149.222.5	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
31.211.102.129	147.237.8.50	Russian Federation	e.tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
163.172.238.45	147.237.77.179	United Kingdom	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
123.206.194.17	147.237.77.179	China	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
58.218.200.137	147.237.76.196	China	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
46.183.223.228	147.237.76.31	Latvia	nakchal.idf.il	ET SCAN Potential SSH Scan	1
42.112.237.25	147.237.77.61	Vietnam	e.cogat.idf.il	ET SCAN NMAP -sS window 4096	1

09-23-2016-00:04:00 to 09-23-2016-01:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.102.242.194	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
185.27.106.147	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
66.249.75.149	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.188	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.25	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
139.59.132.160	Singapore	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
37.142.10.144	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
139.59.132.160	Singapore	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	3
46.19.86.127	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.0.233	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
80.178.130.223	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
77.125.3.221	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	3
84.111.110.206	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
46.116.98.38	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
180.76.15.138	China	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
79.180.62.114	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
46.19.85.25	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
176.13.21.70	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
77.125.3.221	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
37.142.2.168	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	2
217.132.42.253	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	2
37.26.148.184	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
172.56.13.153	United States	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
221.181.73.62	China	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
5.22.134.229	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
77.138.145.42	France	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
141.212.122.85	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
213.57.96.154	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.58	United States	147.237.0.33	idf.il	drop		drop	1
185.20.5.157	United Kingdom	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
46.19.85.15	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
109.253.223.16	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
176.13.0.233	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
24.244.32.102	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
80.178.130.223	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	1
169.229.3.91	United States	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
217.160.182.57	Germany	147.237.77.216	dover.idf.il	Header Rejection	header rejection pattern found in request	monitor	1
77.125.3.221	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.82	United States	147.237.8.28	e.mobile-ks.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
46.19.85.69	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
141.212.122.48	United States	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
37.26.148.184	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
109.66.123.181	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
172.247.85.222	United States	147.237.0.33	idf.il	drop		drop	1
5.29.29.22	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.86	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	1
213.57.145.25	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
63.231.69.145	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.59	United States	147.237.0.33	idf.il	drop		drop	1

09-23-2016-00:04:00 to 09-23-2016-01:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.125.55.32	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
217.132.171.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
109.253.193.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
12.97.17.249	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	2
54.165.230.219	United States	147.237.77.176	matpash.idf.il	Distributed Suspicious Response Code	Block	2
66.249.66.188	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/3/3403.jpg	Block	1
77.139.40.163	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1
46.19.85.25	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
193.19.167.227	Poland	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
66.249.76.71	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/robots.txt	Block	1
46.19.85.92	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	1
207.46.13.174	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/scripts.asmx/getjs	Block	1
66.249.93.72	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
157.55.39.108	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/robots.txt	Block	1
46.121.80.182	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
68.180.231.57	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1115-ar/dover.aspx	Block	1
169.229.3.91	United States	147.237.77.243	mobile.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
46.19.85.25	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 46.19.85.25 (Open Mode)	None	1
180.76.15.16	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/news/jeninkilled/stn	Block	1

09-23-2016-00:04:00 to 09-23-2016-01:04:00