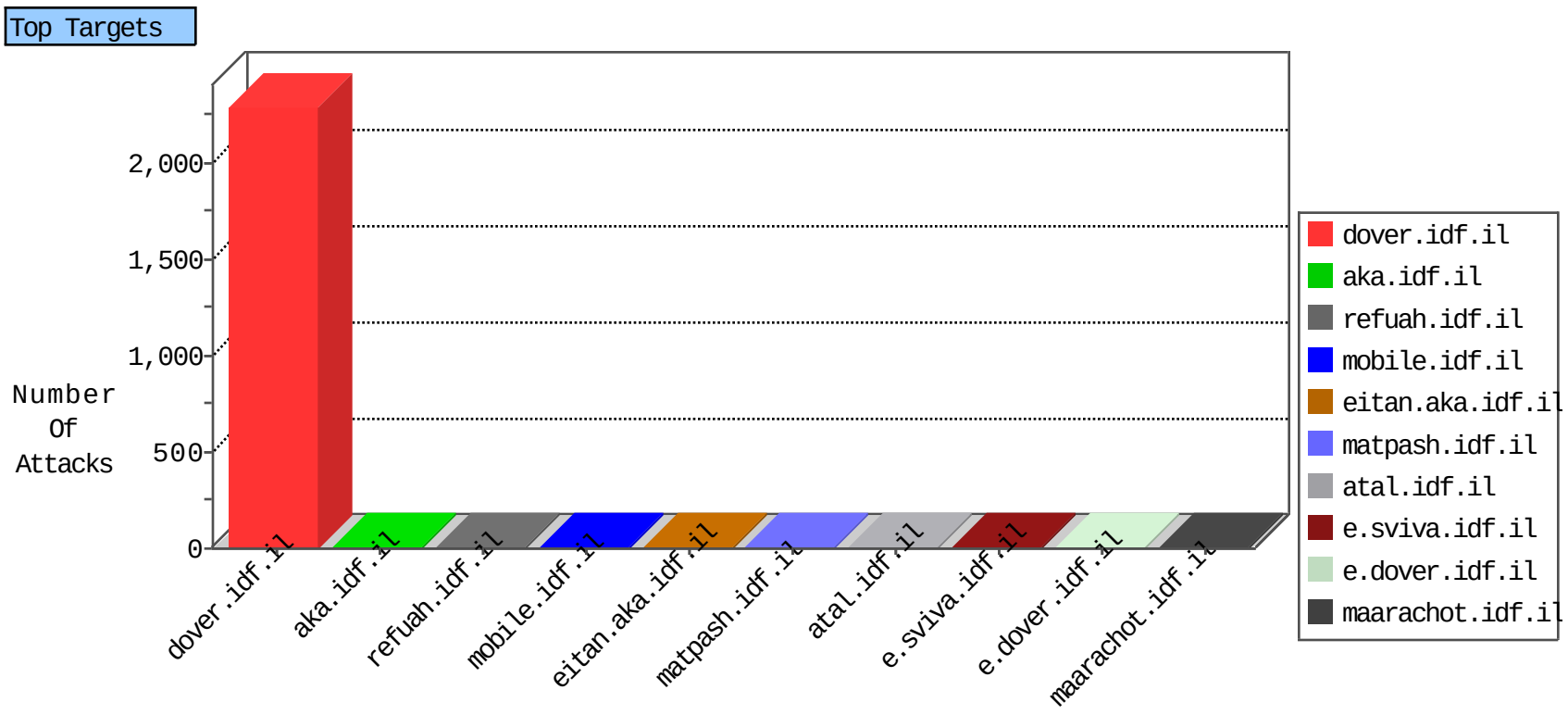
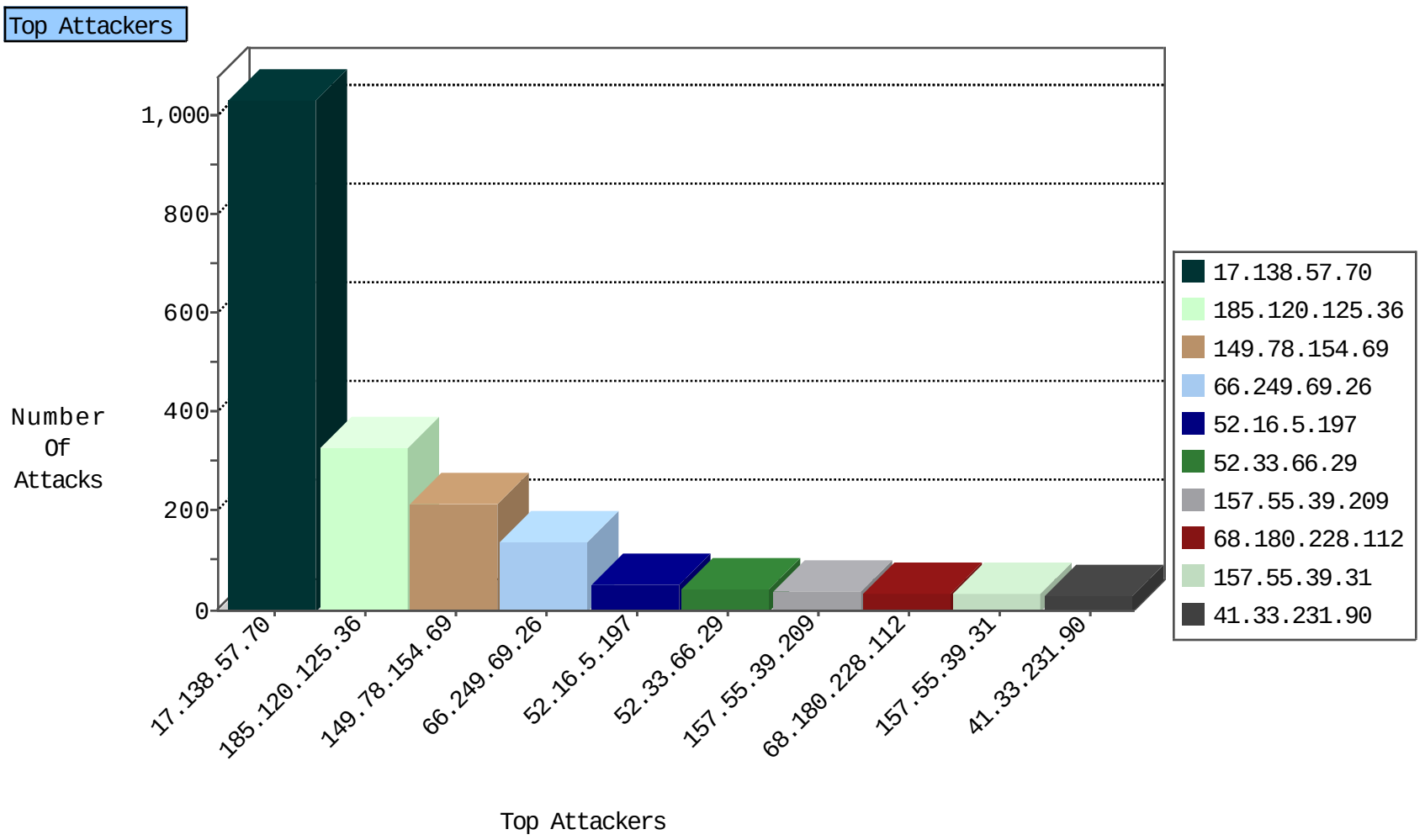
02-13-2016-04:04:09 to 02-13-2016-05:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-13-2016-04:04:09 to 02-13-2016-05:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.54.237	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
61.142.131.111	China	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	2
89.248.174.4	Netherlands	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
31.168.18.60	Israel	147.237.77.170	maarachot.idf.il	Block_Udp_All_Nets	drop	1

02-13-2016-04:04:09 to 02-13-2016-05:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-13-2016-04:04:09 to 02-13-2016-05:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
80.82.64.37	147.237.77.235	Netherlands	sviva.idf.il	ET SCAN Potential SSH Scan	1
80.82.64.37	147.237.77.170	Netherlands	maarachot.idf.il	ET SCAN Potential SSH Scan	1
80.82.64.37	147.237.76.176	Netherlands	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
80.82.64.37	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
31.184.195.114	147.237.77.61	Russian Federation	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.246.0.97	147.237.76.30	China	himush.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.231	147.237.76.39		mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
114.112.90.54	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.0.15	Ukraine	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.64.37	147.237.77.233	Netherlands	atal.idf.il	ET SCAN Potential SSH Scan	1
80.82.64.37	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
80.82.64.37	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
46.151.52.161	147.237.76.38	Ukraine	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.231	147.237.0.15		kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.193	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1

02-13-2016-04:04:09 to 02-13-2016-05:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
82.145.211.19	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	29
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
5.29.32.223	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
199.30.25.93	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
91.200.12.136	Ukraine	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
91.200.12.143	Ukraine	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
66.249.78.230	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
70.39.186.218	Satellite Provider	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	3
130.193.50.14	Russian Federation	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
141.8.132.78	Russian Federation	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
73.184.14.175	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
68.180.229.121	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
70.39.186.222	Satellite Provider	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	2
75.126.221.55	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
184.105.247.240	United States	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
23.242.161.57	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.201	United States	147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.118	United States	147.237.77.243	mobile.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.71.195.222	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
141.212.122.176	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.18	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
23.242.161.57	United States	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
199.168.142.24	United States	147.237.77.170	maarachot.idf.il	drop	SAM rule	drop	1
141.212.122.202	United States	147.237.8.46	e.chinuch.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
218.22.211.69	China	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
185.71.195.222	Iran, Islamic Republic of	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.177	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.32	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
199.168.142.24	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	1
141.212.122.206	United States	147.237.0.35	akaws.idf.il	drop		drop	1
8.37.227.69	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
141.212.122.178	United States	147.237.77.212	e.dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
74.82.47.51	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.113.84	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	1
141.212.122.207	United States	147.237.0.35	akaws.idf.il	drop		drop	1
8.37.227.81	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
198.20.69.74	United States	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.191	United States	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

02-13-2016-04:04:09 to 02-13-2016-05:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
17.138.57.70	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	1017
185.120.125.36		147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	330
149.78.154.69	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	216
66.249.69.26	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	118
52.16.5.197	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	51
52.33.66.29	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	43
157.55.39.209	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	37
68.180.228.112	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	35
157.55.39.31	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	31
208.109.97.62	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	24
50.87.144.145	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	22
192.249.66.247	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	21
2.54.177.45	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	20
66.249.69.26	Israel	147.237.77.216	dover.idf.i	Multiple Unauthorized URL Access from 66.249.69.26	Block	17
17.138.57.70	United States	147.237.77.216	dover.idf.i	Multiple Unauthorized URL Access from 17.138.57.70	Block	16
41.33.232.66	Egypt	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	15
69.149.66.158	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	13
82.80.25.221	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	10
45.35.64.142		147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	8
73.184.14.175	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	8
108.214.86.106	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	6
79.181.117.247	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	4
66.249.91.14	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	4
70.44.227.155	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	4
82.81.40.197	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	4
84.108.105.69	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	4
66.249.69.34	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	4
107.20.36.1	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	4
66.249.69.26	Israel	147.237.77.216	dover.idf.i	Distributed Unauthorized URL Access on www.idf.il/atal1/izkor/view_imgtop.asp	Block	3
109.253.140.54	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
94.159.147.142	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
169.0.183.214		147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
130.193.50.17	Russian Federation	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
85.64.131.4	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
208.69.40.101	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
8.37.227.70	Anonymous Proxy	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
99.112.77.20	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
66.102.7.233	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
107.170.119.178	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
199.203.35.235	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
184.153.75.12	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
72.50.82.94	Puerto Rico	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
8.37.228.81	Anonymous Proxy	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
193.111.255.251	Russian Federation	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
46.121.28.121	Israel	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
108.54.240.96	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
54.167.183.116	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
36.229.217.44	Taiwan	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
104.162.241.87	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2
205.203.135.1	United States	147.237.77.216	dover.idf.i	Distributed Suspicious Response Code	Block	2

02-13-2016-04:04:09 to 02-13-2016-05:04:09