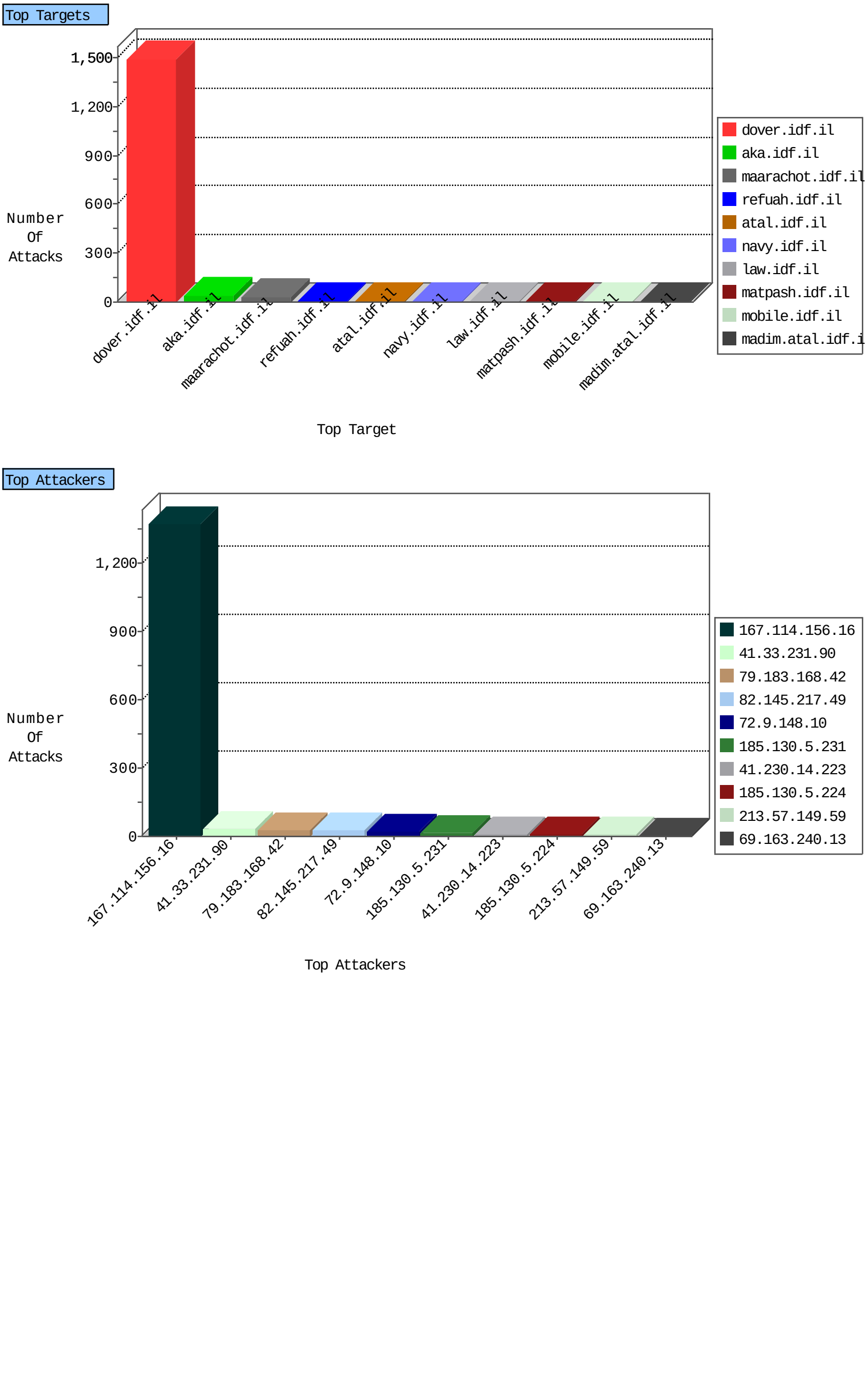
01-02-2016-05:04:02 to 01-02-2016-06:04:02

IDF Under Attack Daily Report



01-02-2016-05:04:02 to 01-02-2016-06:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3030
61.115.220.186	Japan	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1

01-02-2016-05:04:02 to 01-02-2016-06:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

01-02-2016-05:04:02 to 01-02-2016-06:04:02

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	3
66.249.78.199	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
183.60.48.25	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
106.75.199.173	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
93.189.26.18	147.237.77.179	Austria	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.64	147.237.77.179	China	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
185.130.5.224	147.237.76.200		eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
104.143.14.247	147.237.76.42	United States	refuah.idf.il	ET SCAN NMAP -sS window 1024	1

01-02-2016-05:04:02 to 01-02-2016-06:04:02

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	36
79.183.168.42	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	29
82.145.217.49	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	29
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	SAM rule	drop	16
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	drop	SAM rule	drop	12
37.142.220.66	Israel	147.237.77.170	maarachot.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
72.9.148.10	United States	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	4
213.57.149.59	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
208.115.113.84	United States	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
213.57.149.59	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
5.102.254.184	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
40.77.167.75	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.130.249.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
72.9.148.10	United States	147.237.76.86	navy.idf.il	drop	SAM rule	drop	2
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
75.126.221.55	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
185.130.5.231		147.237.77.233	atal.idf.il	drop	SAM rule	drop	2
40.77.167.59	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
185.130.5.231		147.237.77.243	mobile.idf.il	drop	SAM rule	drop	2
77.237.138.202	Czech Republic	147.237.77.121	e.navy.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
157.55.39.76	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
75.126.221.55	United States	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
94.230.86.178	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
77.237.146.28	Czech Republic	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
185.130.5.231		147.237.0.15	kosher-kravi.idf.i	drop	SAM rule	drop	1
185.130.5.224		147.237.76.86	navy.idf.il	drop	SAM rule	drop	1
195.66.76.4	Germany	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
93.189.26.18	Austria	147.237.76.201	e.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
185.130.5.231		147.237.76.197	e.himush.idf.il	drop	SAM rule	drop	1
185.130.5.224		147.237.76.197	e.himush.idf.il	drop	SAM rule	drop	1
52.90.147.70	United States	147.237.77.216	dover.idf.il	Directory Traversal	directory traversal overflow	monitor	1
184.105.247.228	United States	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
101.198.159.31	China	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.130.5.231		147.237.8.28	e.mobile-ks.idf.il	drop	SAM rule	drop	1
185.130.5.224		147.237.76.147	chinuch.aka.idf.il	drop	SAM rule	drop	1
195.154.227.118	France	147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	1
93.189.26.18	Austria	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	1
185.130.5.231		147.237.77.178	e.matpash.idf.il	drop	SAM rule	drop	1
76.114.180.104	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
185.130.5.224		147.237.76.199	e.nakchal.idf.il	drop	SAM rule	drop	1
54.186.248.49	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	1
184.105.247.228	United States	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
5.175.26.46	Germany	147.237.72.166	aka.idf.il	drop	SAM rule	drop	1
141.212.122.174	United States	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
185.130.5.231		147.237.77.235	sviva.idf.il	drop	SAM rule	drop	1
185.130.5.231		147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	1
185.130.5.224		147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	1
184.105.139.76	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

01-02-2016-05:04:02 to 01-02-2016-06:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
69.163.240.13	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 69.163.240.13	Block	5
185.32.179.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.66.20	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1242-he/atal.aspx	Block	1
207.46.13.62	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
84.94.176.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.104	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
52.90.147.70	United States	147.237.77.216	dover.idf.il	URL is Above Root Directory www.idf.il/../shared/clientscripts/jquery/jquery.ticker.js	Block	1
141.212.122.160	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.69.18	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/8/60998.pdf	Block	1
84.111.7.148	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - sigalgs DoS Attack	None	1
66.249.78.111	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/4/60984.pdf	Block	1
52.90.147.148	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
69.163.240.13	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
66.249.73.138	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-16552-en/dover.aspx-title=for	Block	1
54.186.248.49	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
74.82.47.2	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.199	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/aman	Block	1
66.249.66.14	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1244-he/atal.aspx	Block	1
77.237.146.28	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1

01-02-2016-05:04:02 to 01-02-2016-06:04:02