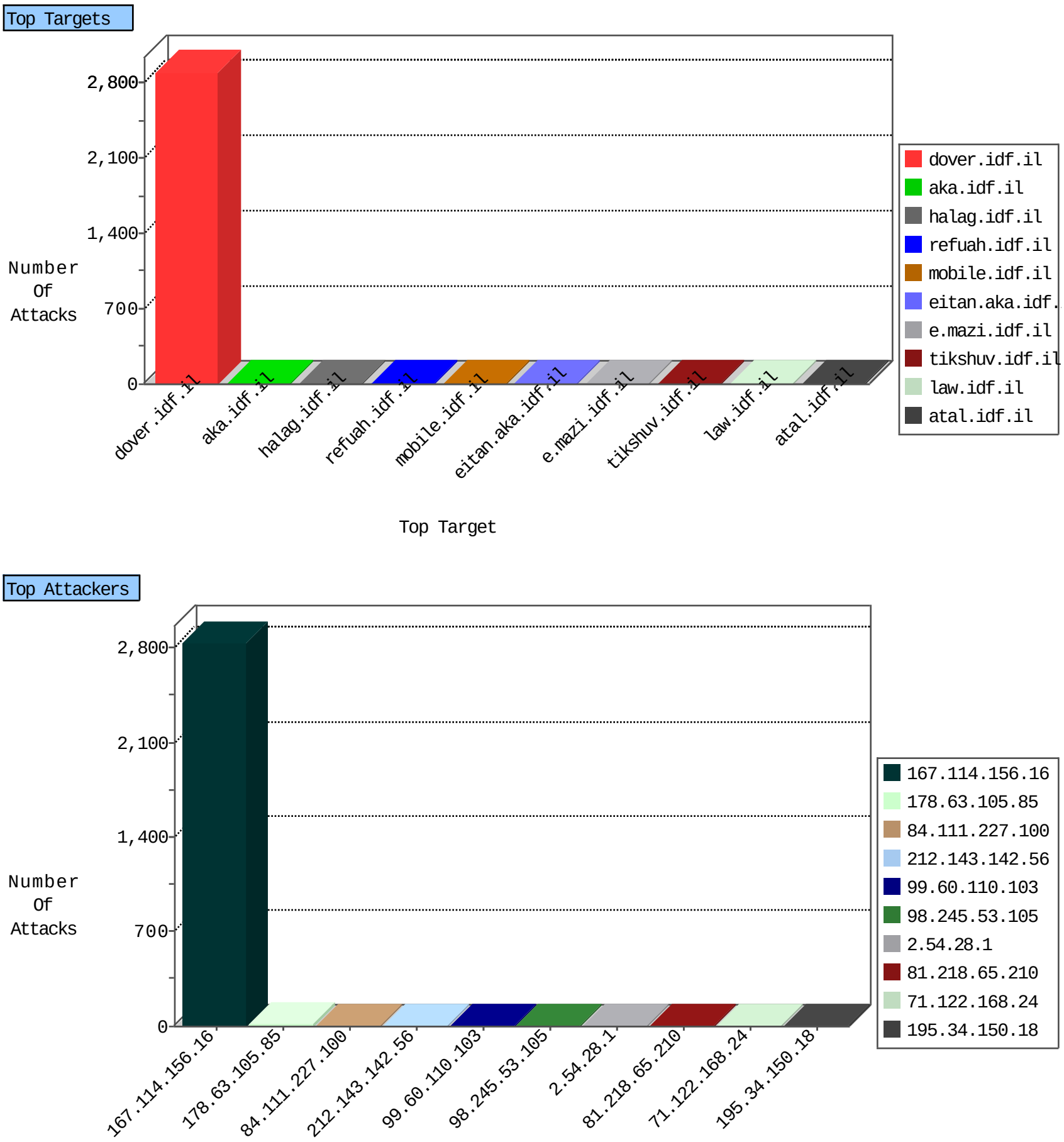
03-16-2016-03:04:09 to 03-16-2016-04:04:09

IDF Under Attack Daily Report



03-16-2016-03:04:09 to 03-16-2016-04:04:09

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	3830
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
182.140.167.188	China	147.237.8.24	e.lifestyle.idf.il	Block_Udp_All_Nets	drop	1

03-16-2016-03:04:09 to 03-16-2016-04:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.149	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
62.212.73.211	Netherlands	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-16-2016-03:04:09 to 03-16-2016-04:04:09

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
104.232.98.38	147.237.77.178		e.matpash.idf.il	ET SCAN NMAP -sS window 2048	1
104.232.98.38	147.237.77.178		e.matpash.idf.il	ET SCAN NMAP -f -sS	1
104.215.89.20	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 2048	1
185.72.179.226	147.237.77.179		e.mazi.idf.il	ET SCAN NMAP -sS window 2048	1
162.243.40.70	147.237.8.14	United States	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
104.232.98.38	147.237.77.178		e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
104.215.89.20	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 4096	1
104.215.89.20	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -f -sS	1
218.246.0.97	147.237.76.200	China	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
185.72.179.226	147.237.77.179		e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
185.72.179.226	147.237.77.179		e.mazi.idf.il	ET SCAN NMAP -f -sS	1

03-16-2016-03:04:09 to 03-16-2016-04:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
99.60.110.103	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
84.111.227.100	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
98.245.53.105	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.54.28.1	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
65.55.210.240	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	4
178.63.105.85	Germany	147.237.77.61	e.cogat.idf.il	drop	SAM rule	drop	4
84.111.227.100	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
24.205.57.72	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.183.169.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.255.215.87	France	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.63.105.85	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	2
178.63.105.85	Germany	147.237.76.176	test.ncore.idf.il	drop	SAM rule	drop	2
178.63.105.85	Germany	147.237.8.45	e.eitan.idf.il	drop	SAM rule	drop	2
178.63.105.85	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	2
178.63.105.85	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	2
178.63.105.85	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	2
178.63.105.85	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	2
216.218.206.82	United States	147.237.77.19	law-forum.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
159.226.95.66	China	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
5.22.131.37	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	1
180.76.15.20	China	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.148	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.7	United States	147.237.77.205	prisha.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.102	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
85.179.162.186	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
8.37.227.69	Anonymous Proxy	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Response out of state	monitor	1
184.105.139.83	United States	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.149	United States	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
74.82.47.20	United States	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
216.218.206.118	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
95.35.127.203	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
184.105.139.88	United States	147.237.8.27	e.madim.atal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
178.63.105.85	Germany	147.237.72.156	aman.idf.il	drop	SAM rule	drop	1
141.212.122.163	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1
46.19.85.53	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.164	United States	147.237.76.148	gqcenter.aka.idf.il	drop		drop	1

03-16-2016-03:04:09 to 03-16-2016-04:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	2
213.57.224.195	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	2
106.68.53.29	Australia	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
68.180.229.124	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8876-he/refuah.aspx	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
207.46.13.105	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
71.122.168.24	United States	147.237.76.42	refuah.idf.il	NULL Character in Method ¬[[#0]][[#0]][[#0]][[#16]]ö[[#11]]–ÒÀeäM%±–	Block	1
216.218.206.66	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to 147.237.76.39/	Block	1
151.55.117.0	Italy	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
68.180.231.39	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-19355-ar	Block	1
211.11.155.20	Japan	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
71.122.168.24	United States	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method ¬[[#0]][[#0]][[#0]][[#16]]ö[[#11]]–ÒÀeäM%±–	Block	1
66.249.78.190	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/headerupper/	Block	1
157.55.39.12	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to www.kosher-kravi.idf.il/templates/shared/usercontrols/headerupper/	Block	1
71.122.168.24	United States	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1283-12738-en/dover.aspx	Block	1
213.57.224.195	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 213.57.224.195	Block	1
84.111.227.100	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.57	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/rights/asp/	Block	1
71.122.168.24	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Method ¬[[#0]][[#0]][[#0]][[#16]]ö[[#11]]–ÒÀeäM%±–	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/yohalan/main/main.asp	Block	1
157.55.39.145	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
71.122.168.24	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in URL	Block	1
66.249.78.102	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
213.57.224.195	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/xmlrpc.php	Block	1
122.109.167.168	Australia	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1

03-16-2016-03:04:09 to 03-16-2016-04:04:09