How the Libraesva URLSand sandboxing service works

What is the Libraesva URLSand sandboxing service

It is a service available on all Libraesva ESG appliances starting with version 4.0. You can enable it in System -> Content Analysis -> Sandbox Filters by checking the “Enable URI Sandbox” checkbox.

This option can be customized for each domain, which means that you can enable it for the whole appliance and disable it for some domain or keep it disabled by default and enable it only for some domain.

How it works

If the option is enabled for the recipient domain, the Libraesva appliance rewrites the URIs it finds inside emails so that when the final recipient clicks on the link it doesn’t go to the original URI but, instead, to the EsvaLabs URI Sanbox service.

Here is an example:

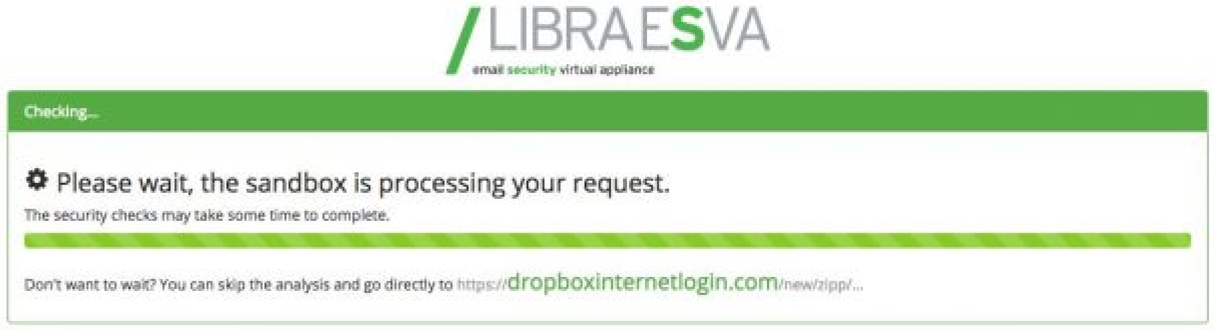
Original URI:
http://www.fivl.it

Rewritten URI:
https://urlsand.esvalabs.com/?u=http%3A%2F%2Fwww.fivl.it&e=366181f3&h=6c12b0dd

When the user clicks on the link, the EsvaLabs URI Sanbox will analyze the target URI in real time by performing lookups on known malware/phishing URI lists and by actively analyzing the contents of the page looking for malicious behavior.

If the URI has recently been analyzed, the response of the Sandbox will be immediate and, if classified as “clean”, and immediate redirect is performed.

If the page has not been recently analyzed, it will be retrieved and scanned, if redirects are found the checks are repeated for all the intermediary URIs. This can take up to a few minutes depending on the number of intermediary pages and the speed of the servers serving those pages.



Checking...

Please wait, the sandbox is processing your request.

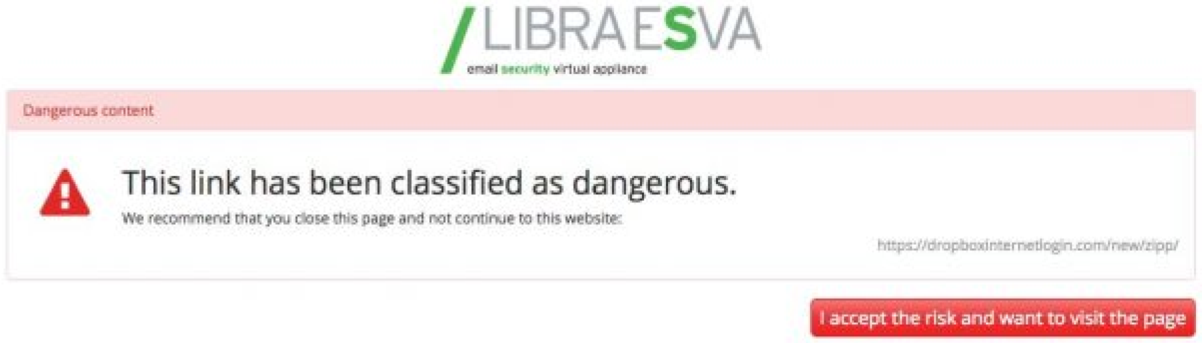
The security checks may take some time to complete.

Don't want to wait? You can skip the analysis and go directly to https://dropboxinternetlogin.com/new/zipp/...

The user is allowed to skip the checks but warned about it, and the complete URI is shown to allow the user to decide whether to trust it or not.

Here is an example of a legit URL.

If the URI is classified as “dangerous” a blocking page is displayed.


LIBRAESVA
email security virtual appliance
I accept the risk and want to visit the page

Dangerous content

This link has been classified as dangerous.

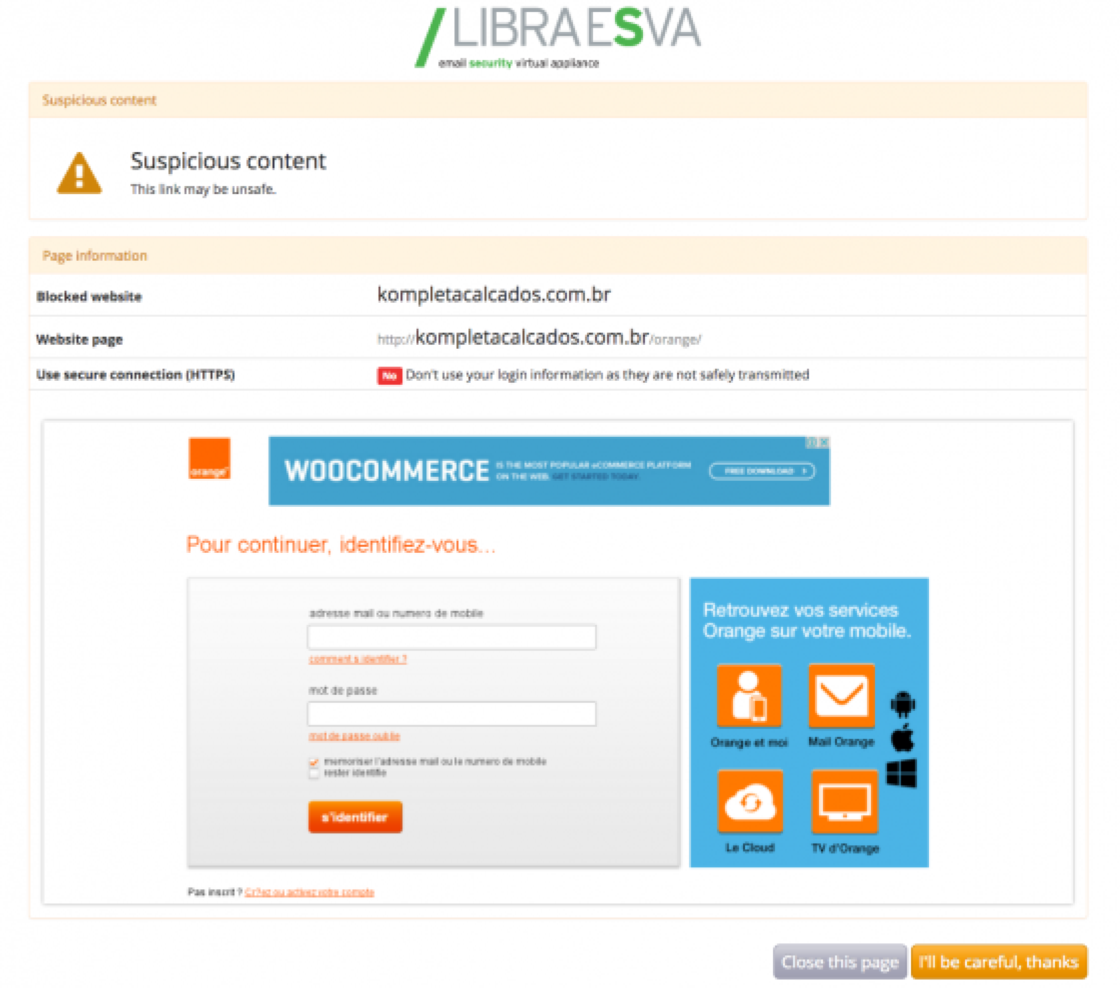
We recommend that you close this page and not continue to this website:

https://dropboxinternetlogin.com/new/zipp/

The option “I accept the risk and want to follow this dangerous link” can be disabled with the Libraesva ESG configuration flag “Do not allow users to skip URI Sandbox checks”.

Here is an example of a malicious URL.

If the URI is classified as “suspect” a warning page with the website screenshot preview is displayed to allow visual checks of the requested website.



LIBRAESVA
email security virtual appliance

Suspicious content

Suspicious content
This link may be unsafe.

Page information

Blocked website	kompletacalcados.com.br
Website page	http://kompletacalcados.com.br/orange/
Use secure connection (HTTPS)	No Don't use your login information as they are not safely transmitted

orange
WOOCOMMERCE IS THE MOST POPULAR eCOMMERCE PLATFORM ON THE WEB. GET STARTED TODAY
FREE DOWNLOAD

Pour continuer, identifiez-vous...

adresse mail ou numero de mobile
comment s'identifier ?
mot de passe
mot de passe oublie
☑ memoriser l'adresse mail ou le numero de mobile
□ rester identifie
s'identifier

Retrouvez vos services Orange sur votre mobile.
Orange et moi
Mail Orange
Le Cloud
TV d'Orange

Pas inscrit ? Créez ou activez votre compte

Close this page
I'll be careful, thanks

The option to show suspect website preview to the user can be disabled with the Libraesva ESG configuration flag "Show preview for suspicious pages".

Here is an example of a suspicious URL.

Privacy

We gather the absolute minimum amount of information we need to provide the service. In the rewritten URI you can see that there are only three parameters:

- The original URI
- A unique ID of the Libraesva ESG appliance that has rewritten the URI
- A checksum that guarantees the integrity of the data

The last two parameters are required to verify that only legit URIs are processed by the service (i.e. URIs rewritten by Libraesva ESG appliances) and that the URI has not been tampered with.

The identity of the recipient of the email is not provided to the Sandbox. Of course the original URI may contain parameters that could identify the recipient, this is inevitable. For example, a URI to unsubscribe from a mailing list might contain the email address of the recipient.

The Sandbox service is accessed via HTTPS which protects the whole conversation between the user’s browser and the sandboxing service.

The Sandbox engine may forward the requested URI to external services to improve the detection.

Exceptions

Libraesva provides and maintains a list of exceptions via it’s usual update service. This list instructs the ESG appliance not to rewrite URIs that match these exception list. Only highly reliable services where no user content is available are included in such list.

The administrator of the Libraesva ESG appliance can add exceptions via System -> Content Analysis -> Impersonation Protection > Phishing Highlight > Phishing Sites List table. All URIs for the sites added as “safe” to the “Phishing Sites List” are not rewritten.