Phishing alert on ZIMBRA

An e-mail from **« adquisiciones@fadu.edu.uy »** is sent to Zimbra users notifying them that their password has expired. They are then asked to change their Zimbra password, with the option of keeping the same password by redirecting them to a login page.

The ultimate goal of this campaign is to recover Zimbra users' access accounts and passwords.

The recovered data can be used to access not only work-related e-mail, but also other accounts (social networks, online banking, other e-mail addresses), as users often reuse the same password for different services.

Here is the link in question:

- *hxxps://tfb.intrabench.com/?redirect&__CONFIRM=11111.myZOJSzidI.383&REDIRECT=T&__URL=http://gouv.tg.2EbT.d3rpsqu4d[.]net/a?Y2luYS5sYXdzb25AZ291di50Zw==*

[Warning, do not click on the link]

Tip 1: DO NOT click on the link.

Tip 2: In case you clicked on the link

- **Call CERT.tg on 22-53-59-80 or report the incident on www.cert.tg**
- **Change all your passwords on all your accounts**
- **It is recommended to use different passwords for each type of account.**

Tip 3: A password management tool can be used to manage your passwords.

Tip 4: For administrators

- **Ensure that indicators of compromise (IOCs) are not present.**
- **If IOCs are present, ensure that recommendations are effectively implemented**
- **Make users aware of best practices**

Indicators of compromise:

- *adquisiciones@fadu.edu.uy*
- *gouv.tg.2ebt.d3rpsqu4d[.]net*
- *d3rpsqu4d[.]net*
- *hxxps://tfb.intrabench.com/?redirect&__CONFIRM=11111.myZOJSzidI.383&REDIRECT=T&_URL=http://gouv.tg.2EbT.d3rpsqu4d[.]net/a?Y2luYS5sYXdzb25AZ291di50Zw==*
- *IP : 162.241.124.47*