Automatic cleanup of email for the enduser

Because everyone uses Gmail and bitcoins are expensive.

CIRCL
Computer Incident
Response Center
Luxembourg

Raphaël Vinot - *TLP:WHITE*

July 5, 2016

Current status

- "Do not click on stuff in emails from people you don't know"
- "Discard all exe attachments"
- "Do not run macro"

Does it works?

- Nope
- Nope
- Nope
- Nope

Let's think about it

- When do you receive macros in your personal mailbox? An exe? A javascript?
- You don't have your own mailserver and/or don't want to give a mail to everyone you know
- What about an IMAP proxy?

Existing code

- Mark as malicious all active content
- Unpack and process archives
- Everything happens in memory
- Attaches logs
- Mail $\rightarrow$ Script $\rightarrow$ Mail

TODO

- Write the actual IMAP proxy
- $\Rightarrow$ https://github.com/OfflineIMAP/imapfw
- Take a nap

Q&A

- `https://github.com/CIRCL/PyCIRCLeanMail`
- We welcome new functionalities and pull requests.