

COPPER CROW has recently been attacking your industry and companies just like yours. Luckily, you work for a company where their Cyber Defense team has been working to build some solid detection and already have some detection rules in place!

Last Friday, you noticed an alert for a phishing email that looked suspicious. The Incident Response Team has been working to ensure that employees aren’t compromised, but they need you to look at the attached document to validate the information and to see if there is further malware or actions that they should be looking out for.

## Sample Location:

<https://drive.google.com/file/d/1QJZhgB_0thjGJgqqHNzhCy7OQa4IKn2d/view?usp=sharing>

(Password: infected)

## Challenge Deliverable

For this challenge, we would like you to create a malware report for invoice-02-01-2022.xls.

## Need Help?

* Slack
* If you have any questions, please send an email to [cyber.challenges@target.com](mailto:cyber.challenges@target.com)

## Analysis Tools

* CyberChef
  + The Cyber Swiss Army Knife - a web app for encryption, encoding, compression and data analysis
  + <https://gchq.github.io/CyberChef/>
* Oletools
  + Python tool to analyze Microsoft OLE2 files, such as Microsoft Office documents
  + <https://github.com/decalage2/oletools>
* Python
  + <https://github.com/mandiant/speakeasy>
* Speakeasy
  + Speakeasy is a portable, modular, binary emulator designed to emulate Windows kernel and user mode malware.
  + <https://github.com/mandiant/speakeasy>