

# Thomas FERRY

## Veille technologique:

Maison de retraite à Marigny Le Lozon

A dark blue diagonal gradient bar that starts from the bottom left corner and extends towards the top right corner, covering the lower half of the slide.

# Sommaire:

- Qui
- Où
- Quand
- Par qui
- Pourquoi
- Comment
- Conséquences
- Réactions et Solutions
- Sources

# Qui?

-La victime de l'attaque fut une maison de retraite EHPAD nommée "Les Hortensias"



# Où?

L'attaque s'est passée à Marigny-le-Lozon, près de Saint-Lô, en  
Manche, qui se situe en Normandie.



Quand?

L'attaque s'est passée le  
23 Octobre 2023

# Par Qui?

Medusa, un groupe de cybercriminels,  
fut derrière l'attaque.



# Pourquoi?

Medusa ayant demandé une rançon de 100000\$, leur motivation était très probablement l'argent



# Comment?

Pour s'infiltrer dans le réseau, Medusa a commencé par utiliser la technique du Phishing (ou hameçonnage), qui consiste à envoyer un mail tout en se faisant passer pour une compagnie, existante ou non.

Ce mail représente soit une commande "Accidentelle" soit une fausse facture ou une amende, pour pousser l'utilisateur à cliquer sur le lien

Voici à Droite quelques exemples de Phishing



Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: \$135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

<http://www.trustedbank.com/general/custverifyinfo.asp>

Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

Thank you,  
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

## Scammers are impersonating Geek Squad

Report  
impersonator scams at  
**ReportFraud.ftc.gov**



FEDERAL TRADE  
COMMISSION



DATE : 09-08-2022

Dear User,

Your Subscription with GEEK SQUAD will Renew Today and \$349.99 is about to be Debited from your account by Today. The Debited Amount will be reflected within the next 24. In case of any further clarifications or block the auto-renewal service please reach out Customer Help Center.

Customer ID: [REDACTED]

Invoice Number: YDGC9873

Description Quantity Unit Price Total Geek Squad Best Buy Service (One Year Subscription)

Subtotal \$349.99

Sales Tax \$0.00

Total \$349.99

If you didn't authorize this Charge, you have 24 Hrs. To cancel & get an instant refund of your annual subscription, please contact our customer care: [REDACTED]



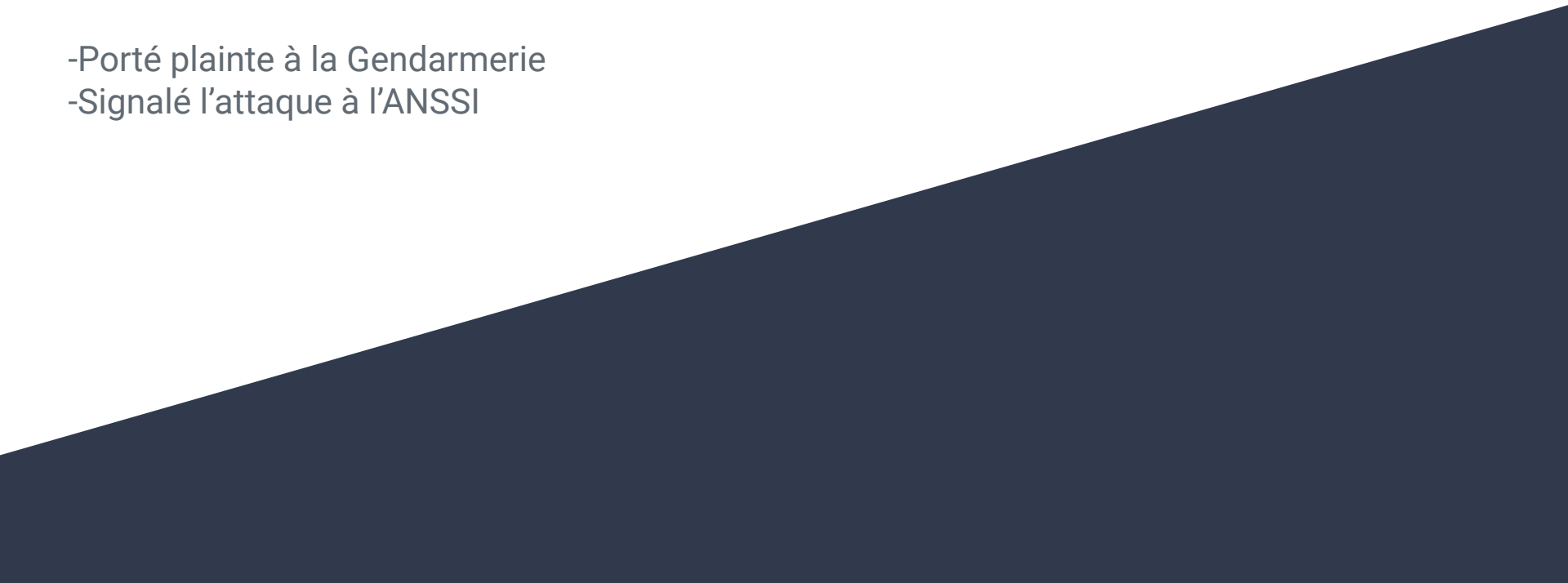
# Comment? (Partie 2)

Après que l'utilisateur tombe dans le panneau en cliquant sur le lien, Medusa aura la capacité d'infiltrer le réseau, et d'y injecter son code, et donc son logiciel de rançon, qui encrypte les données et demandera une rançon

# Conséquences

Certains fichiers ont déjà été diffusés sur le "darknet", des cartes d'identité notamment, mais aussi des documents internes d'organisation ou des factures, les serveurs informatiques étaient inutilisables. Quatre ordinateurs étaient également totalement bloqués.

# Réaction et Solutions

- Porté plainte à la Gendarmerie
  - Signalé l'attaque à l'ANSSI
- 
- A dark blue diagonal gradient bar that starts from the bottom left and extends towards the top right, covering the lower half of the slide.

# Sources

Ouest France :

<https://www.ouest-france.fr/normandie/marigny-le-lozon-50570/une-maison-de-retraite-en-normandie-victime-dune-cyberattaque-84e9d906-7312-11ee-8ee4-6d23d2858b34>

France Bleu :

<https://www.francebleu.fr/infos/faits-divers-justice/manche-l-ehpad-de-marigny-le-lozon-victime-d-une-cyberattaque-des-donnees-des-residents-devoilees-5237559>