セキュリティレポート

2023.6

YOU DESERVE THE BEST SECURITY

2023年から急増している Microsoft OneNote形式のファイルを悪用した攻撃

手軽に文字入力や画像、ファイルを添付することができ、最近中小企業で利用が増えているOneNote。

こちらを悪用した攻撃が今年に入ってから急増しています。

もしかしたら**『ウチはOneNote使ってないよ！』**という方も少なくないと思いますが、下記の**攻撃手法**まで読んでくださいね！

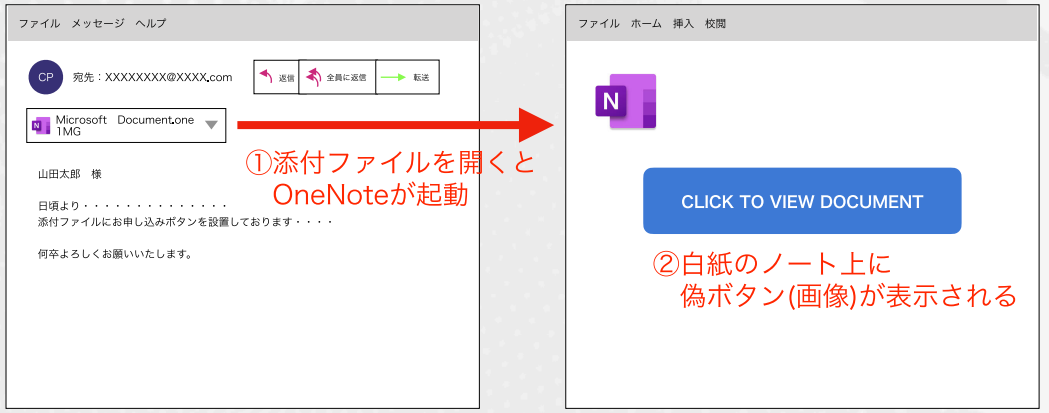
攻撃手法 (IPA調べ)

まず攻撃者はOneNote形式のファイルを添付したメールを送付

ファイル名には、請求書配達通知、注文書などに関係するものが記載されている事が多く、
メールの本文には、添付ファイルの開封を促す内容が記載されていることが多い。

添付ファイルを開くと、ノートにはボタンや文書ファイルのアイコンをクリックするように促す指示が書かれている。これらのアイコンは本物ではなく、特定の位置を示すものとなっている。

受信者がアイコン（の位置）をダブルクリックすると。ノートに埋め込んだ悪意のあるファイルが実行され、受信者のコンピュータをウイルスに感染させる。



③ 偽のボタンをクリックすることで、
悪意あるファイルが実行されてしまう

CHECK POINT

対策はどの様にすれば？？

見極め方

- ✦ノートの内容が、見えない状態(白紙、不鮮明)になっている
- ✦ノートに「CLICK TO VIEW DOCUMENT」「View」「Open」等のボタンが表示されている
- ✦ノートに文書ファイルのアイコンが表示されている
- ✦ノートの内容や添付されている文書ファイル、クラウドサービス上のファイルを閲覧するために、ボタンやファイルのアイコンをクリックするように促す指示が書かれている

身近に出来ること

- ◆ 身に覚えのないOneNote形式のファイルは開かない
- ◆ 身に覚えのないOneNote形式のファイルのノートに書かれた指示には従わない
- ◆ OneNote形式のファイルの閲覧中に、セキュリティ警告が表示された際、警告文をよく確認し、安全であると判断できない場合は「OK」ボタンをクリックしない

CHECK POINT

フィッシング対策にはクラウドセキュリティ Harmony!!

◆ 以前に比べ「怪しいメール」を判断しづらい
◆ メール経由の標的型攻撃やランサムウェア等の攻撃が増えた
◆ パスワード付き添付ファイルの検査ができない

今回の様なNTTファイナンスの事案も含め、メールを経由した攻撃は後を断ちません。一昔前までは、『怪しいメールを開かない』という声掛けで防いでいましたが、
現在は見分けがつかず巧妙化し、被害も拡大しています。

これらを解決する**『Harmony Email & コラボレーション』**は

◆ 悪質な添付ファイルをブロック
◆ ゼロフィッシング対策
◆ パスワード付きファイルの検査
◆ アノマリー検知

機能を備える、クラウド型アドバンストメールセキュリティとして、
悪意あるメールから企業を守ります!!

悪質な添付ファイルをブロック

・添付ファイルを無害して提供
・バックグラウンドでファイルをスキャン、悪質な場合はブロックします

ゼロフィッシング

数秒で300以上の指標を分析、フィッシングサイトを判定します

パスワード付きファイル検査機能

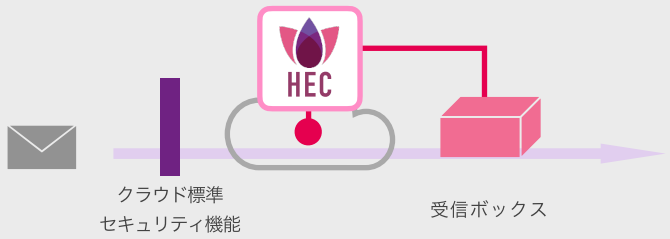
今後増加が予想されるパスワード付きZipファイルによる添付マルウェアも検査可能

アノマリー（異常行動）検知機能

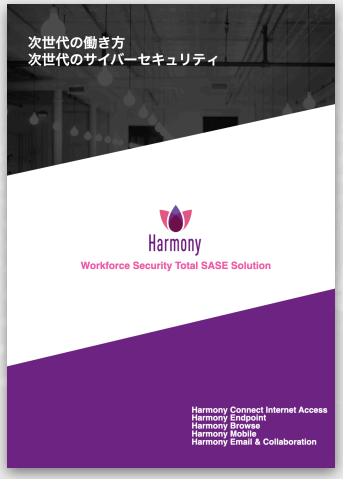
普段と違う国からのメールや、不自然なメールの大量送付などによる異常行動を検知します

Harmony
Workforce Security Total SASE Solution

Harmony Email & Collaboration



- 攻撃者が迂回できないセキュリティ対策
- クラウド標準セキュリティ機能との併用可
- AI / MLベースのセキュリティ対策
- クラウドサービス内容に組み込まれたAPI型セキュリティ
- 他のAPI型製品では対応できない、受信前のセキュリティ検査が可能



フィッシング対策には

Harmony Mobile
Harmony Browseも

効果を発揮します!!

Harmonyシリーズの
デジタルカタログは
https://cp-smb.com/catalog

CHECK POINT