フィッシング攻撃 vs Minerva Armor（Minerva Labs 社の製品名）
2021 年 9 月 26 日のブログから

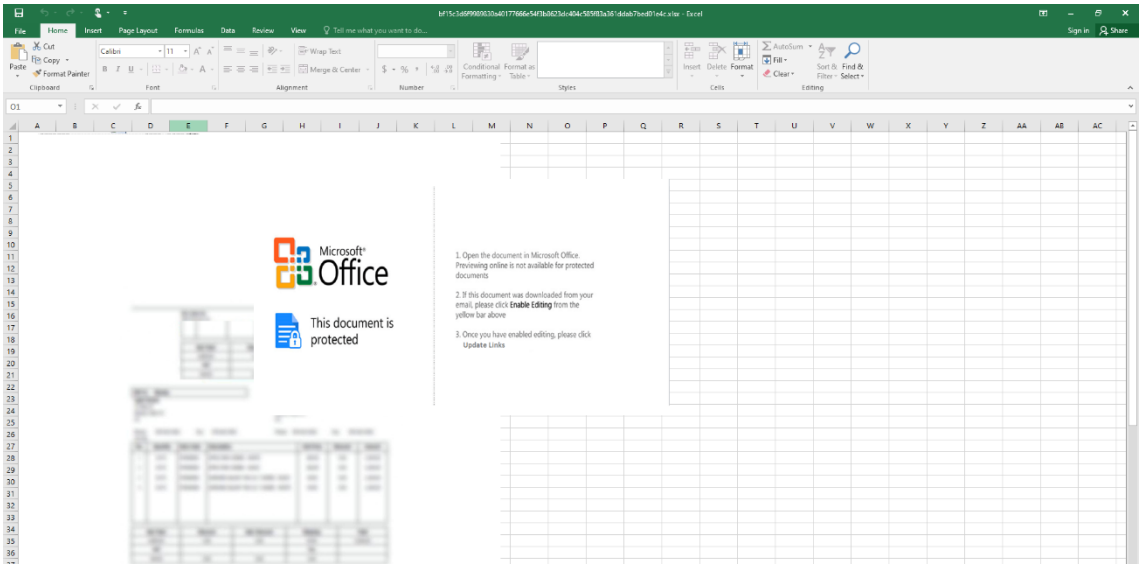
近年におけるサイバー攻撃者の多くが以前よりも増して高度になりました。企業組織のネットワーク上でサイバー攻撃を受けた場合の多くは攻撃の最終段階で既に少なからず損害を受けていることでしょう。サイバーキルチェーンにおいて最も重大なステージの一つがマルウェアの不正侵入です。

長年にわたり多くのマルウェア侵入経路として最たる手法がフィッシング攻撃と言えるでしょう。この攻撃手法はソーシャルエンジニアリング（人間の心理的な隙や、行動のミスにつけ込んで個人が持つ秘密情報を入手する手法）で偽のメールなどを利用し相手の隙をついて重要な情報又は企業組織のネットワークへの不正侵入のセキュリティホールを開放してしまいます。

2021 年のある統計によると、少なくとも 91%のサイバー攻撃がフィッシング攻撃という報告があります。エンドユーザーはこのような悪質化していくサイバー攻撃チェインの犠牲者と化します。

フィッシング攻撃は以下のように仕掛けられます。

- Email – メール添付ファイルに悪意のあるドキュメント又は URL のリンク先が掲載
- Website – 健全なウエブサイト(Paypal, Ebay など)の偽物ログインページ
- SMS – 偽のウエブサイトや悪意のあるダウンロードページへ誘導
- Twitter, Facebook や LinkedIn などの SNS – 偽のログインページを囮として個人パスワード情報を盗んだり、求職者の履歴書ファイルに悪意のあるマクロを仕掛けダウンロードさせる手法



フィッシング攻撃の典型的な仕掛け手法はメール上に偽の請求書ファイルを添付などですが、昨年はコロナ蔓延に関するメールに Excel/Word ファイル添付され、悪意のあるマクロが仕掛けられているケースです。T この悪意のマクロはリモートコマンド・コントロールサーバー(C&C Server)から悪意のあるマクロがダウンロードされクリックすると実行されます。

LCG Kit や EtterSilent などの正当なツールを利用して攻撃を仕掛けたりします。
典型的なフィッシング攻撃で登場するマルウェアとして Trickbot, Emotet, Ursnif などです。Minerva の先制防御テクノロジーで Microsoft Office 製品が悪意のあるペイロードと実行を下の図に示すように先制防御します。

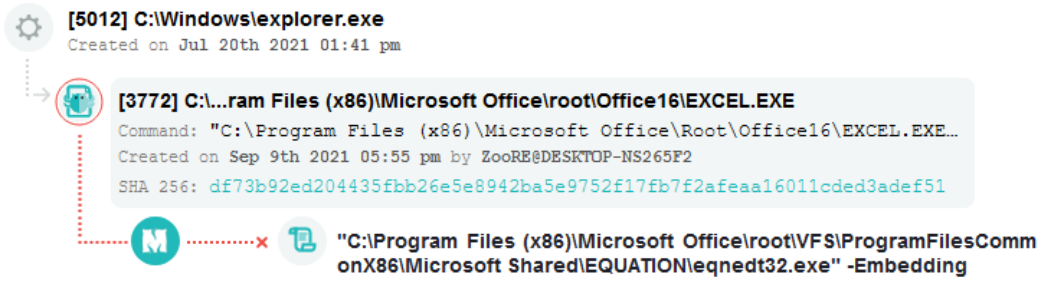


図 1 – 悪意の EXCEL ファイルが eqnedt32.exe を利用して任意コードを実行するのを先制防御した攻撃タイムライン

Minerva 製品(Minerva Armor)についてのお問い合わせは Pico Technologies (info@pico-t.co.jp)までお願い致します。