新たな DatopLoader（Squirrelwaffle）で QakBot を送り込む
2021 年 11 月 9 日 Minerva のブログから

新たなフィッシング攻撃手法として DatopLoader（別名:Squirrelwaffle）を利用して Qakbot 感染させる手口を見てみましょう。

DatopLoader（別名:Squirrelwaffle）はマルスパム（スパムメールでマルウェア付きのファイル）経由で侵入を試み、標的のネットワークへ攻撃の足掛かりをつくります。攻撃者はさらに侵入に成功することで他のマルウェアも送り込み複数感染させることで被害者から金銭窃取を狙うという訳です。

Yesterday (November 8, 2021), we spotted a malicious excel file trying to execute three different files using regsvr32.exe:2021 年 11 月 8 日に、Minerva リサーチチームは、悪意のあるエクセルファイルが regsvr32.exe を利用して3つの異なるファイルが攻撃実行しようとしました。

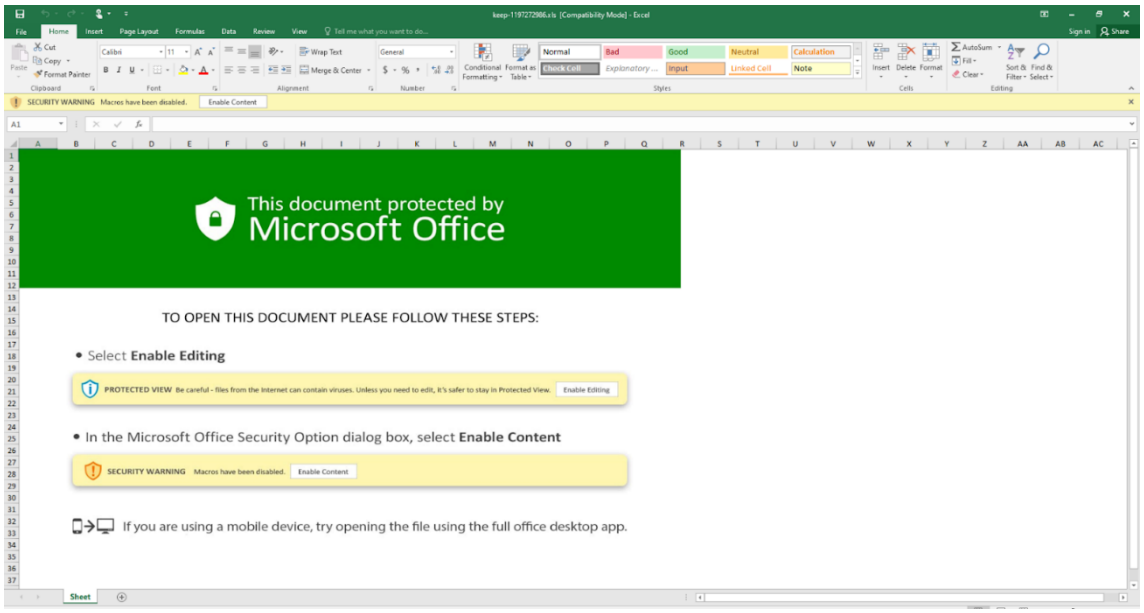
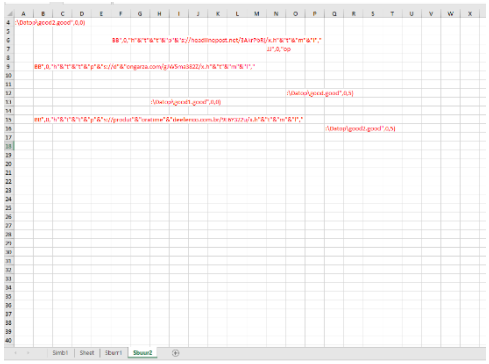
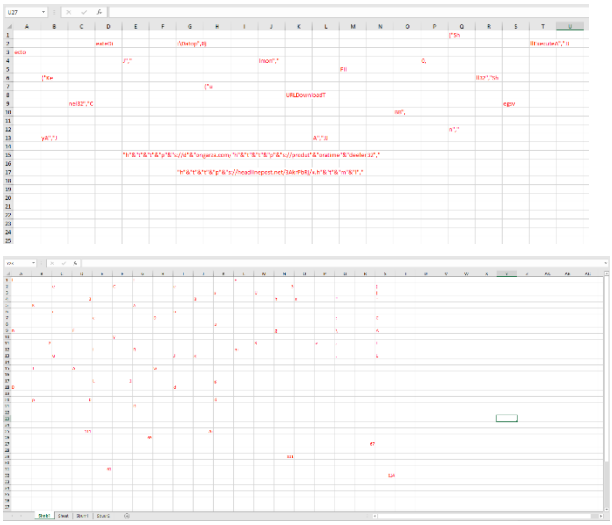


図1　悪意のあるエクセルファイル

まず初めに、このエクセルファイルはマクロの実行前の画面です。実行してしまうとネットワークが侵入され最終的に Qakbot などが送り込まれます。このシートは何ら悪意のファイルには見えませんが、実は危険なファイルなのです。実証実験として Developer Tab を有効にして、VBA プロジェクトでこのファイルをチェックすることにしました。

3つのエクセルシートが隠されており、可視モードへ切り替えました。3 つの全てのシートは共通に Excel Macro 4 が含まれており、1 つのシートには、文字、数字、シンボルが含まれており、他の 2 つのシートはどうやら kerner32.dll!CreateDirectoryA を利用し、新規フォルダーを生成するような仕組みとなっていました。3 つの事なるドメインからそれぞれのファイルがダウンロードされることにより、新規フォルダーが生成されローカルディスク上に3つのファイルが保存され、各ファイルは regsvr32.exe を利用して攻撃を実行するのです。





- C:¥の下に生成された新規フォルダーは Datop という名前で保存される
- ダウンロードされたファイルは C:¥Datop¥good.good, C:¥Datop¥good1.good and C:¥Datop¥good2.good.という名前で保存される

これら3つのダウンロードされたファイルは Qakbot というバンキングトロイの DLLs であることが判明しました。この Qakbot は Pinkslipbot, Qbot 又は Quakbot という名でも知られています。この悪名高いトロイの木馬は、アクセス認証情報やオンラインバンキングの情報などを窃取し、最終的にはアカウント自体を乗っ取ってしまいます。Squirrelwaffle は以下の図に示されている同経路で送り込まれていることが分かります。

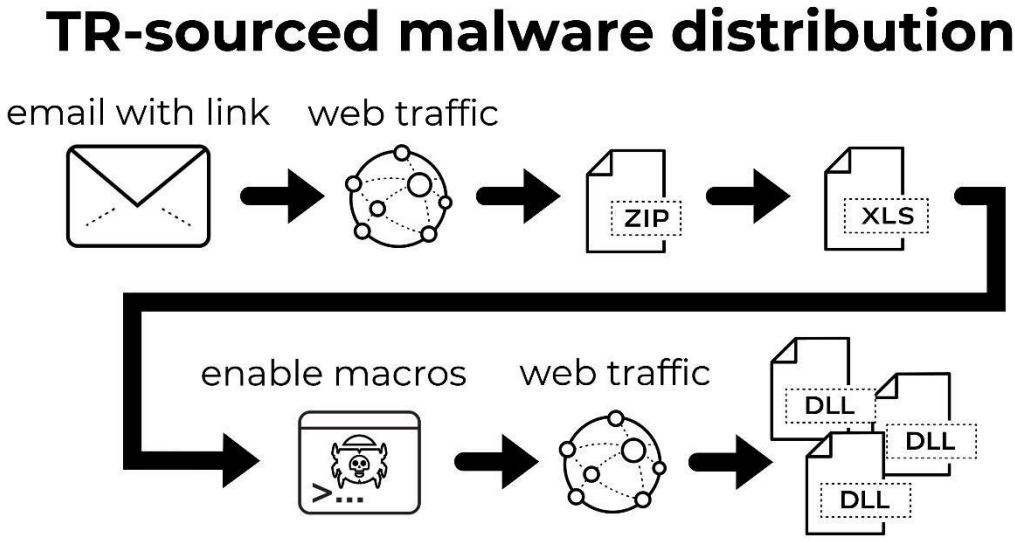
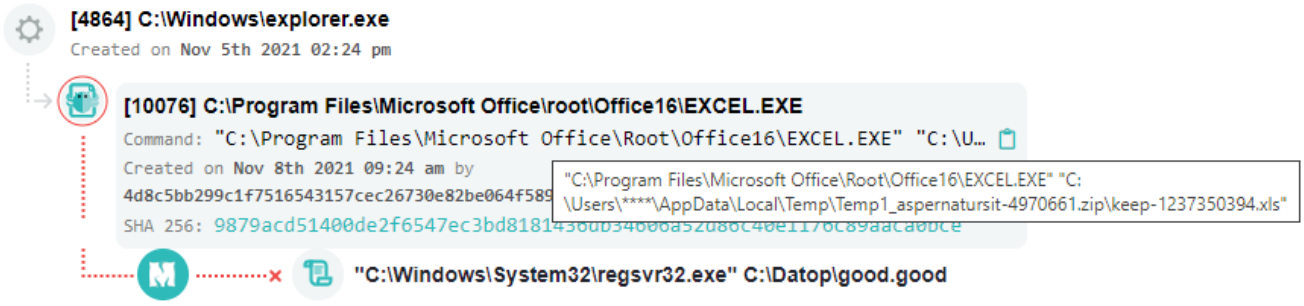


図 2 Squirrelwaffle が送り込まれる感染経路図

Minerva の悪意のあるドキュメント防御モジュールは Squirrelwaffle タイプのマルウェアを先制防御しますので企業を狙った大規模な感染を完全シャットアウトします。



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。