Trickbot ギャングメンバー2 名が逮捕されるが、Trickbot マルウェアは蔓延中
2021 年 10 月 10 日 Minerva のブログから

Trickbot マルウェアは 2016 年から付き合っています。これはバンキングのトロイの木馬で金融機関とユーザーをターゲットにバンキングデータを盗みとります。長年にわたりこのマルウェアは複合モジュラーへと進化を遂げ Windows と Linux 両方に感染が広がっていきました。

Trickbot マルウェアは、ネットワークへ侵入後、攻撃実行しランサムウェアがインストールされることから、Conti ランサムウェアと統合されたかのように思われがちです。他の Trickbot マルウェアについては、BazarLoader と呼ばれ Ryuk ランサムウェアを仕掛けていました。

特に環境技術関連の企業、オンライン教育企業、米国バーモント大学のヘルスケアネットワークなどへランサムウェア攻撃が仕掛けられました。通常 Trickbot マルウェアは、フィッシング攻撃などで、メールに貼り付けてある URL や添付ファイルに悪意のマルウェアが仕掛けられています。

Trickbot のルーツですが、ロシアが拠点とされていると疑われています。最近そのグループ

メンバーの 1 人が韓国滞在中に摘発されました。容疑者はラトビア国籍で Trickbot のギャングメンバーを新規ランサムウェアのプラットフォームを開発及び提供した容疑で米国司法省から起訴されました。しかしこの逮捕劇に関わらず、Trickbot は現在も進行形の状態です。先日、the Malwarebytes Threat Intelligence チームが新規のフィッシング攻撃キャンペーンを発見したとツイートして注意勧告をしています。現在も連鎖攻撃が進行しています。

1. 被害者はメール添付のドキュメントファイルを開き、悪意のあるマクロが起動してしまいました。

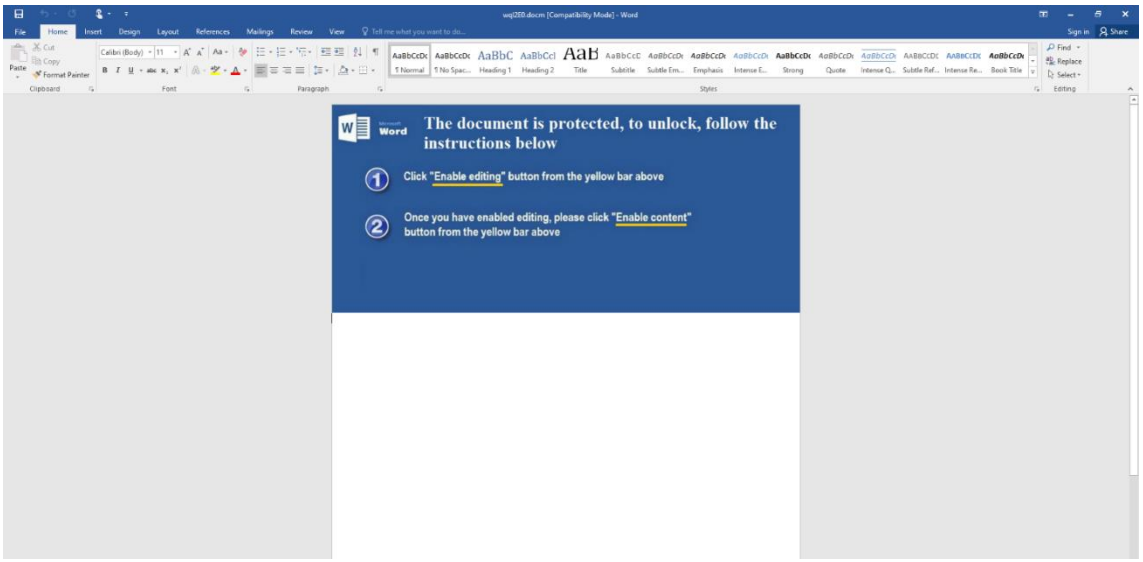

図 1 悪意のあるドキュメントファイル

1. 被害者がマクロを実行してしまうと.bat ファイルと呼ばれるファイルがランダムに C:¥ProgramData directory へドロップしてしまいます。

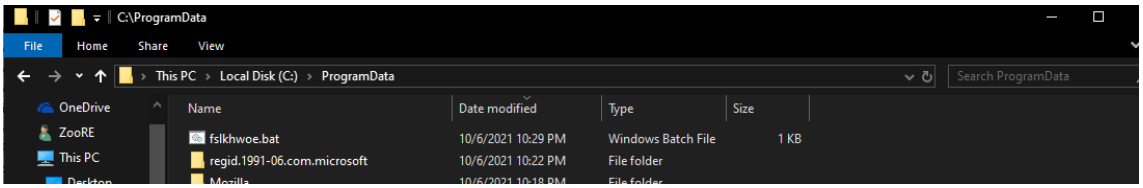

図 2.bat ファイルドロップの様子

1. 攻撃者サーバーから Trickbot ペイロード攻撃が開始され、PowerShell を利用し.dll ファイルとして C:¥ProgramData へドロップされる。

2. サイバー攻撃注意勧告サイト T1218.011 MITRE technique 上に WinWord が rundll32.exe を利用して悪意のある DLL を実行する。

3. サイバー攻撃注意勧告サイト T1055.012 MITRE technique 上に悪意のある DLL が svchost.exe へインジェクション攻撃を実行する。

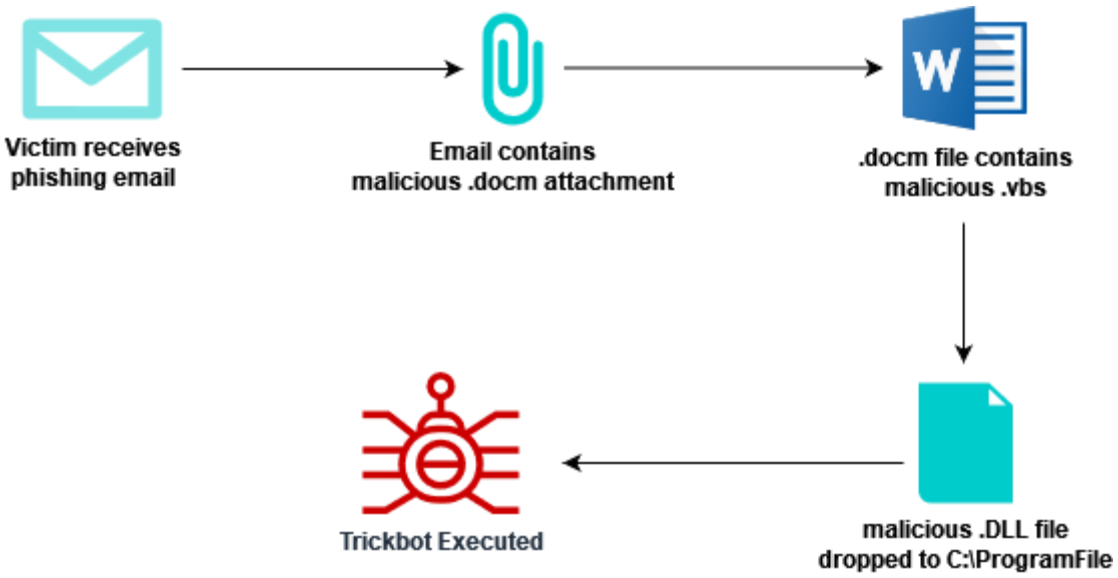

図 3 攻撃実行のプロセスフロー

ギャングは新たなツールを開発及び既存ツールをアップグレードして持続的に攻撃武器を進化しています。Minerva のマクロ攻撃防御テクノロジーはドロップ防御と Trickbot ファミリーに属するマルウェアの攻撃実行を先制防御します。

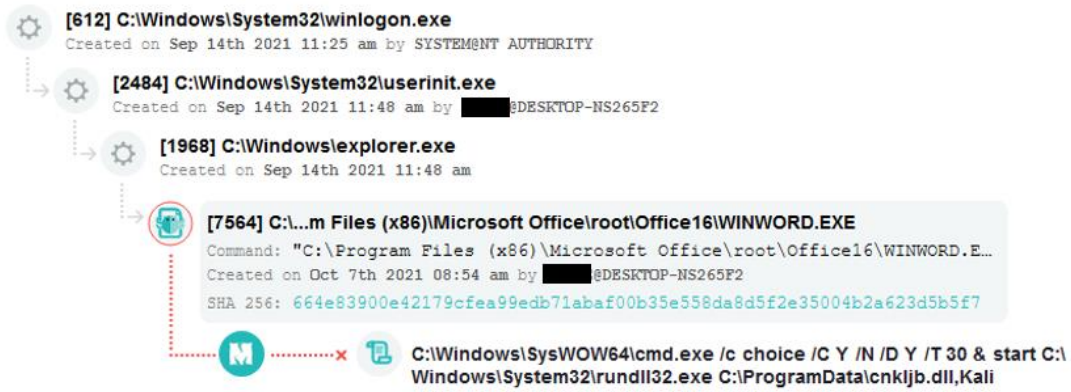

Figure 4 Trickbot Malware Executed Prevented

図 4 Trickbot 攻撃防御

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。