報道関係者各位

インフォスティーラー『DUCKTAIL』による被害が拡大、1 件あたり数十万米ドルの被害に

～ 今夏以降、攻撃手法がより進化し、より巧妙に ～

2022 年 11 月 24 日
ウィズセキュア株式会社

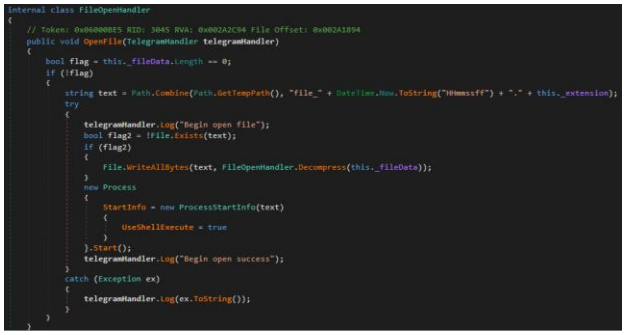
先進的サイバーセキュリティテクノロジーのプロバイダーである WithSecure (旧社名: F-Secure、本社: フィンランド・ヘルシンキ、CEO: Juhani Hintikka、日本法人: 東京都港区、以下、ウィズセキュア) は、同社が本年 7 月に発見した[*1]、ベトナムのサイバー攻撃者グループによるインフォスティーラー型マルウェア『DUCKTAIL』による被害が拡大し、1 件あたりの被害額が数十万米ドルになるケースも出ていると警告を発しました。

2021 年の活動開始後、DUCKTAIL は企業などの Facebook 広告／ビジネスアカウントの管理権限を持つと推測される従業員の LinkedIn ページを経由して、Facebook アカウントを乗っ取ることを目的に活動してきました。本年夏にウィズセキュアが発表したレポートで DUCKTAIL の活動が明らかになりましたが、その後もこのサイバー攻撃者グループは防御をかいくぐり、活動を拡大するためにその手法を進化させています。

ウィズセキュアのリサーチ部門である WithSecure Intelligence (略称: WithIntel) のリサーチャーを務める Mohammad Kazem Hassan Nejad (モハマッド・カゼム・ハッサン・ネジャッド) は、今夏以降の DUCKTAIL の活動について次のように語っています。
「DUCKTAIL が直ちに減速する兆候は見られず、むしろ運用上の困難に直面しつつも急速に進化していると私たちは考えています。これまで DUCKTAIL を背後で運用するサイバー攻撃者グループは小規模なのでと考えられてきましたが、その規模は拡大しているようです。」

本年 9 月上旬以降に観測された DUCKTAIL の活動で観測された動作モードの変化:

- ターゲットにフィッシングを仕掛けるために WhatsApp などの新たなルートを使用
- より「正規のアドレスである」と感じさせるメールアドレスを取得し、起動時にダミーの文書や動画ファイルを開くことで、マルウェアをより正規のものに見せかけるという機能の強化
- ファイル形式やコンパイルの変更、証明書の連名化など、防御回避策の強化
- ベトナムで多くのフェイク企業を立ち上げ、関連会社をオペレーションに組み込むことで、さらなるリソースの開発とオペレーションを拡大



```
internal class FileOpenHandler
{
    // Token: 0x06000BE5 RID: 3045 RVA: 0x002A2C94 File Offset: 0x002A1894
    public void OpenFile(TelegramHandler telegramHandler)
    {
        bool flag = this._fileData.Length == 0;
        if (!flag)
        {
            string text = Path.Combine(Path.GetTempPath(), "file_" + DateTime.Now.ToString("HHmmssff") + "." + this._extension);
            try
            {
                telegramHandler.Log("Begin open file");
                bool flag2 = !File.Exists(text);
                if (flag2)
                {
                    File.WriteAllBytes(text, FileOpenHandler.Decompress(this._fileData));
                }
                new Process
                {
                    StartInfo = new ProcessStartInfo(text)
                    {
                        UseShellExecute = true
                    }
                }.Start();
                telegramHandler.Log("Begin open success");
            }
            catch (Exception ex)
            {
                telegramHandler.Log(ex.ToString());
            }
        }
    }
```

(ダミーファイルを起動するためのコードスニペット)

ウィズセキュアのバイスプレジデントであり WithIntel の責任者を務める Paolo Palumbo (パオロ・パルンボ) は、今後の DUCKTAIL の動向について、こう述べています。
「ランサムウェア攻撃は注目を集めていますが、DUCKTAIL のような脅威はターゲットとなる企業に金銭的にも評判においても大きな損害を与えることとなり、看過できないものとなっています。活動の活発化、新しい関連会社やフェイク企業により、今後しばらくは DUCKTAIL 関連のインシデントの増加が予想されます。」

ウィズセキュアのインシデントレスポンスチームは、DUCKTAIL やその他の Facebook の広告／ビジネス向けプラットフォームをターゲットとした脅威による攻撃への対応において、被害を受けた多くの企業にサポートを提供してきました。これまでの DUCKTAIL の攻撃による損失は、10 万米ドル～60 万米ドル相当の広告クレジットと広範囲にわたっています。

(チャネルに送信された暗号化された流出ファイルの例)

Facebook の使用において個人アカウントとビジネスアカウントが分離されていないため、企業にとって管理は困難となります。ウィズセキュリティのインシデントレスポンス部門のグローバル責任者である John Rogers (ジョン・ロジャーズ) は、アカウント管理の難しさについて以下のように次のように話しています。
「同じリソースをプライベートとビジネスの両方で使用することは、非常に大きな問題があります。例えば、DUCKTAIL のインシデントの可能性を調査する際、個人の Facebook の履歴に関するログが必要になることがありますが、これは業務上、倫理上、法律上、予期せぬ多くの問題を引き起こす可能性があります。これは組織とその従業員に関連する事項なので、両者ともこうした状況でのリスクを理解する必要があります。」

以下、ウィズセキュアが DUCKTAIL および類似の脅威からの防御において推奨するステップです:

- Facebook/Meta のビジネスアカウントの管理権限を持つユーザーに対し、フィッシングに関する啓発を行う
- 未知のファイルを実行できないようにするために、アプリケーションの許可リストを強制的に作成
- EDR/EPP ソリューションを使用し、攻撃ライフサイクルの初期段階でマルウェアを予防／検知
- 企業の Facebook アカウントで使用される管理デバイスや個人用デバイスは、基本的なセキュリティハイジーンと保護がなされていることを確認
- Facebook Business アカウントにアクセスする際は、プライベートブラウジングを使用して各作業セッションを認証 (終了後にセッションが切れるため、Cookie が盗まれたり悪用されたりするのを防止)
- Meta が推奨するセキュリティ対策に従う
- インシデントが疑われる場合の対応では、関連するログをできるだけ早くダウンロード／分析

リサーチの内容 (英語) は以下のページにてご覧いただけます:
https://labs.withsecure.com/publications/ducktail-returns

*1:
https://www.withsecure.com/jp-ja/whats-new/pressroom/20220726-ducktail

WithSecure Web サイト:
https://www.withsecure.com/jp-ja/

WithSecure プレスページ:
https://www.withsecure.com/jp-ja/whats-new/pressroom

WithSecure™について

WithSecure™は、IT サービスプロバイダー、MSSP、ユーザー企業、大手金融機関、メーカー、通信テクノロジープロバイダー数千社から、業務を保護し成果を出すサイバーセキュリティパートナーとして大きな信頼を勝ち取っています。私たちは AI を活用した保護機能によりエンドポイントやクラウドコラボレーションを保護し、インテリジェントな検知と対応によりプロアクティブに脅威を検出し、当社のセキュリティエキスパートが現実世界のサイバー攻撃に立ち向かっています。当社のコンサルタントは、テクノロジーに挑戦する企業とパートナーシップを結び、経験と実績に基づくセキュリティアドバイスを通じてレジリエンスを構築します。当社は 30 年以上に渡ってビジネス目標を達成するためのテクノロジーを構築してきた経験を活かし、柔軟な商業モデルを通じてパートナーとともに成長するポートフォリオを構築しています。
1988 年に設立された WithSecure は本社をフィンランド・ヘルシンキに、日本法人であるウィズセキュア株式会社を東京都港区に置いています。また、NASDAQ ヘルシンキに上場しています。
詳細は www.withsecure.com をご覧ください。また、Twitter @WithSecure_JP でも情報の発信をおこなっています。

主要ソリューション:

WithSecure™ Elements Endpoint Detection and Response (EDR)
WithSecure™ Cloud Protection for Salesforce
サイバーセキュリティコンサルティング