Secureworks®

脅威インテリジェンス エグゼクティブレポート

Volume 2022, Number 4

カウンター・スレット・ユニット™（CTU）
リサーチチーム

エグゼクティブサマリー

セキュアワークスのカウンター・スレット・ユニット（CTU™）リサーチチームは、セキュリティの脅威を分析し、企業や組織のシステム保護を支援しています。2022年5月から6月にかけて世界全域で観測された脅威動向をもとに、注目すべきポイントをCTU™のリサーチャーがまとめました。

- **国家支援型の攻撃グループにも利用されるランサムウェア**
- **無防備なデータが狙われる**
- **ランサムウェア攻撃と同程度の被害をもたらすビジネスメール詐欺（BEC）**

国家支援型の攻撃グループにも利用されるランサムウェア

ランサムウェア攻撃は金銭目的だけとは限りません。別の動機で発生することもあります。

ランサムウェアのエコシステムは刻々と変化しています。次々と登場しては消える亜種は、わずか数社にダメージを与えただけで消滅する場合もあります。ランサムウェア攻撃の大半は金銭目的のより広範囲な活動ですが、他の動機を示唆する活動パターンも見られます。こうした脅威動向の進化に目を光らせることは、当社CTUリサーチチームの重要な任務です。

当社CTUのリサーチャーは5つのランサムウェアファミリーのクラスタを特定し、これらの運営元が中国の攻撃グループBRONZE STARLIGHTであることを確認しました。5つとも短期間で消滅しており、加盟メンバー（Affiliate）の関与はありませんでした。また、同一のコードや「HUI Loader」と呼ばれるローダーマルウェアが使用されている、という共通点もありました。

このほか、中国政府が支援する攻撃グループBRONZE RIVERSIDEによる知的財産（IP）窃取攻撃でも、HUI Loaderが使われていました。いずれの攻撃グループも同じツール（HUI Loader）を使用していることから、BRONZE STARLIGHTとBRONZE RIVERSIDEにはつながりがあることが示唆されます。したがって、BRONZE STARLIGHTは金銭目的ではなく、知的財産窃取およびサイバースパイ活動を目的とした国家支援型の攻撃グループである可能性があります。

イランや北朝鮮などで活動する国家支援型の攻撃グループの間でもランサムウェアが用いられていますが、動機は様々です。北朝鮮の場合は、制裁を迂回しつつ同国経済に必要な資金を調達するための金銭目的である可能性が高いものの、イランの場合はランサムウェアを装った破壊的かつ不可逆的な暗号化を行うことが多いです。

こうした事実からも、インシデント対応時に潜在的な影響をくまなく定量化できるよう、「攻撃意図」を把握することがいかに重要であるかが改めてわかります。

上記を踏まえ、ぜひ実行してほしいアクション：
自社が保有するデータを把握し、誰が当該データに関心を持つのか把握しておきましょう。また、インシデント対応チームやベンダーが最新の脅威インテリジェンスにアクセスできる状態を整えておきましょう。

「無防備なデータ」が狙われる

安全でない場所に社内データが放置され、外部アクセス可能な状態になっているケースがあまりにも多く見られます。インターネット上で広く出回っているツールを使えば、こうしたデータはいとも簡単に発見され、攻撃グループに侵害されてしまいます。

当社CTUのリサーチャーは2022年6月、1,200を超えるElasticsearchデータベースに、「データを復元してほしければビットコインで身代金を払え」という内容の身代金要求文が挿入されていたことを確認し、報告しました。被害の対象はすべて、インターネット公開されている認証が不要なデータベースでした。当初は大規模な攻撃かと思われましたが、こうした脆弱なデータをすぐに特定できるインターネット検索ツール（無料で使用でき、使いやすいShodanなど）の存在を考えれば、驚くことではありません。

このように、脆弱なデータベースを攻撃しデータの窃取や恐喝を試みる手口は広く蔓延しています。広範囲に攻撃を行うグループにとって、窃取可能なインターネット公開データを特定するための検索を行うことは比較的簡単です。

多くの組織は「ごく小数の正規ユーザーでない限り、社内資産の保管場所を特定したり、資産にアクセスしたりすることは難しいだろう」という誤った思い込みのせいで、重要な社内資産のセキュリティを適切に確保できていません。このほか、「API認証キーをGitHubなどの公開リポジトリに格納したまま放置する」というのもよくある失敗です。攻撃者はこの点を熟知しており、認証キーを特定・窃取するためのフリーツールの操作にも長けているため、API認証キーは常に非公開環境に格納しておくべきです。

上記を踏まえ、ぜひ実行してほしいアクション：
公開状態のデータベースについては、その要否（インターネット公開の必要性）を今一度見直し、公開する必要がある場合は多要素認証を実装しましょう。また、当該データベースのデータ資産へのアクセスを自動付与するAPIキーが誤って外部に露出しないよう、保護しましょう。

ランサムウェア攻撃と同程度の被害をもたらすビジネスメール詐欺（BEC）

ランサムウェア攻撃は大きく報道されますが、実際の被害額はグローバルで見ると、その件数の多さからビジネスメール詐欺（BEC）のほうがランサムウェア攻撃を上回っています。ビジネスメール詐欺の件数は増加の一途をたどり、偽装の精度もさらに高まっているため、早期根絶は難しいでしょう。

ナイジェリア警察は今年5月、インターポールのOperation Delilah作戦の一環として、ビジネスメール詐欺グループSilverTerrier/TMTのリーダーと見られる人物を逮捕しました。同グループは2015年に発生したビジネスメール詐欺事案にも関与しており、これまで4大陸にまたがる何千もの法人および個人が被害に遭っています。

ビジネスメール詐欺の攻撃グループは2022年に入っても、10年前と同じ攻撃手法を用いていることが当社CTUのリサーチャーによって確認されています。同じ手口を使い続ける理由は「効果があるから」です。BECの手口で一番多いものは、ユーザーのメールアカウントの侵害です。セキュリティ対策に不備がある組織を狙えば素早く簡単にユーザーアカウントを侵害できるほか、攻撃用のマルウェアを開発したり展開したりする必要もありません。こうした攻撃で被害を受けた場合、損失額は100万ドルを優に超えることもあります。

BEC攻撃では、テクノロジー面だけでなくビジネスプロセスも標的になります。そのため、支払い取引を実行する前に内容を慎重に精査する財務統制プロセスの整備が不可欠です。テクノロジー面での統制も、対策として有用です。多要素認証の実装によって攻撃を回避でき、ログの確認によって不正ログインや異常なメール転送ルール追加を検知できます。

BEC攻撃を受けると、甚大な金銭的被害に遭う可能性があります。当社のインシデント対応コンサルタントは常に、メールセキュリティを確保することおよび、BEC攻撃でよく使われる偽装ドメイン（ドメインスプーフィング）を監視することを、企業や組織の皆様に推奨しています。

上記を踏まえ、ぜひ実行してほしいアクション：

- Microsoft 365などのプラットフォームへのアクセス時の多要素認証を実装しましょう。
- 監視ツールの対象範囲にクラウドインフラのデータが含まれていることを確認しましょう。
- 高額な支払い処理の検証・承認に関する社内ビジネスプロセスを検証しましょう。

結論

サイバー攻撃の中には簡単に実行できるものもあります。例えば、標的の候補を探索することができるツールは容易に入手できます。有効な防御策を実現させるには、ビジネスプロセス設計とテクノロジー実装の両面で、常にセキュリティを最優先に据える必要があります。また、脅威動向に関する専門家の知見や最新の状況を把握することも重要です。

CTUリサーチチームについて

CTUのリサーチャーは、メディアでも頻繁に取り上げられ、セキュリティコミュニティ向けの技術分析を公開し、セキュリティカンファレンスでは新たな脅威について説明しています。セキュアワークスの高度なセキュリティテクノロジーと、業界でのネットワークを活用して、CTUリサーチチームは脅威アクターを追跡し、異常なアクティビティを分析して、新しい攻撃手法と脅威を追跡しています。このプロセスにより、CTUのリサーチャーは、脅威をすぐに識別し、損害が生じる前にお客様を保護する対策を開発します。

リサーチ
お客様が直面する脅威の根本を理解し、対処・保護するための対策を作成

インテリジェンス
ネットワークエッジを超えて、脅威の可視性を強化する情報を提供

統合
CTUによるリサーチとインテリジェンスを、セキュアワークスのマネージド・セキュリティ・サービスとコンサルティングに投入

Secureworks®

Secureworks® (NASDAQ: SCWX) は、サイバーセキュリティにおける世界的な先進企業です。当社ソリューションをご活用いただくことにより、お客様やパートナーは攻撃者よりも常に先手を打ち、マーケットに迅速に対応し、ビジネスニーズを満たすことができます。クラウドネイティブのSaaSセキュリティプラットフォームとインテリジェンス主導のセキュリティソリューションの独自の組み合わせにより、20年以上の脅威インテリジェンスと分析から得た深く広い知見を提供しております。このように、長年にわたるサイバー攻撃の最前線で蓄積した実践経験に基づく知見を提供するセキュリティプラットフォームは、唯一無二のセキュアワークスだけです。

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
www.secureworks.com

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs Forest, Sydney NSW Australia 2086

日本
〒100-8159
東京都千代田区大手町一丁目2番1号
Otemachi Oneタワー17階
www.secureworks.jp

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdo

1 Tanfield
Edinburgh EH3 5DA
United Kingdom

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111

緊急のインシデント対応に関するご相談は、こちらまでご連絡ください。

03-6848-9760

