アラート (AA20-099A) : COVID-19 サイバー攻撃者による悪用

〇概要

これは、米国国土安全保障省(DHS)サイバーセキュリティ・インフラセキュリティ庁(CISA)と英国の国家サイバーセキュリティセンター(NCSC)からの共同アラートです。

このアラートは、現在のコロナウイルス病 2019(COVID-19)グローバルパンデミックのサイバー犯罪者および高度な永続的脅威(APT)グループによる搾取に関する情報を提供します。検出のための侵害の指標 (IOC) の包括的なリストと軽減のアドバイスが含まれています。

CISA と NCSC の両方が、悪意のあるサイバーアクターによる COVID-19 関連のテーマの使用が増加しています。同時に、テレワーキングの急増により、仮想プライベートネットワーク(VPN)などの潜在的に脆弱なサービスの利用が増加し、個人や組織に対する脅威が増大しています。

APT グループやサイバー犯罪者は、COVID-19 関連の詐欺やフィッシングメールを使用して、個人、中小企業、大規模な組織を標的にしています。このアラートは、COVID-19 関連の悪意のあるサイバー活動の概要を提供し、個人や組織が影響を受けるリスクを軽減するために従うことができる実用的なアドバイスを提供します。このアラートの添付ファイル .csv および .stix 内に提供される IIC は、CISA、NCSC、および業界の分析に基づいています。

注:これは動きの速い状況であり、このアラートは、すべての COVID-19 関連の悪意のあるサイバー活動をカタログ化しようとはしません。個人や組織は、COVID-19 に関する活動の増加に対して警戒を続け、自らを守るための積極的な措置を講じる必要があります。

〇技術内容

【攻撃の概要】

APT グループは、サイバー事業の一環として COVID-19 パンデミックを使用しています。これらのサイバー脅威アクターは、多くの場合、信頼できるエンティティを装います.彼らの活動には、コロナウイルスをテーマにしたフィッシングメッセージや悪意のあるアプリケーションの使用が含まれており、以前に侵害された可能性のある信頼できるエンティティを装うことが多

い。彼らの目標と目標は、スパイ活動や「ハッキング・アンド・リーク」作戦などの長年の優先事項と一致しています。

サイバー犯罪者は、商業的利益のためにパンデミックを使用しています, ランサムウェアやその他のマルウェアの様々な展開.

APT グループとサイバー犯罪者の両方が、今後数週間から数ヶ月にわたって COVID-19 大流行を引き続き利用する可能性が高い。観察される脅威は次のとおりです。
・コロナウイルスまたは COVID-19 の件名をルアーとして使用したフィッシング
・コロナウイルスまたは COVID-19 をテーマにしたルアーを使用したマルウェアの配布
・コロナウイルスまたは COVID-19 に関連する文言を含む新しいドメイン名の利用
・新しく(そしてしばしば急速に)展開されたリモート アクセスおよびテレワーキング インフラストラクチャに対する攻撃

悪意のあるサイバーアクターは、基本的なソーシャルエンジニアリング方法に依存して、ユーザーに特定のアクションを実行するように誘導します。これらのアクターは、潜在的な犠牲者を説得するために、コロナウイルス大流行の周りの好奇心や懸念などの人間の特徴を利用しています:
リンクをクリックするか、フィッシング Web サイト、またはランサムウェアを含むマルウェアのダウンロードにつながる可能性のあるアプリをダウンロードします。たとえば、悪意のある Android アプリは、リアルタイムのコロナウイルスアウトブレイクトラッカーを提供することを目的としていますが、代わりにユーザーをだまして"CovidLock"ランサムウェアをデバイスにインストールするための管理アクセスを提供しようとします。[1]

マルウェアを含むファイル (電子メールの添付ファイルなど) を開きます。たとえば、電子メールの件名には、「コロナウイルスアップデート」や「2019-nCov:あなたの街でコロナウイルスの流行(緊急)」などの COVID-19 関連のフレーズが含まれています。

真正性の印象を作り出すために、悪意のあるサイバーアクターは、電子メールで送信者情報を偽装して、世界保健機関(WHO)やタイトルに「Dr.」を持つ

個人などの信頼できる情報源から来ているように見せかけることができます。いくつかの例では、サイバー攻撃者は偽の電子メールログインページへのリンクを含むフィッシングメールを送信します。他の電子メールは、組織の人事 (HR) 部門からのものであると考え、添付ファイルを開くように従業員にアドバイスします。
マルウェアペイロードを含む悪意のある添付ファイルは、「プレジデントは、Cabinet.rtf とコロナウイルスによる予算削減について議論する」など、コロナウイルスまたは COVID-19 関連のテーマで命名される可能性があります。

注:このアクティビティに関連する Ioc の完全なリストは、このアラートの .csv ファイルと .stix ファイルに含まれています。

【フィッシング】
CISA と NCSC はどちらも、上記のソーシャル エンジニアリング手法を使用する大量のフィッシングキャンペーンを実施しています。

フィッシングメールの件名の例は次のとおりです。
・2020 コロナウイルスのアップデート,
・コロナウイルスのアップデート,
・2019-nCov: あなたの都市で新たに確認されたケース、
・2019-nCov:あなたの街でコロナウイルスの流行(緊急事態)。

これらの電子メールには行動の呼びかけが含まれ、悪意のあるサイバーアクターがユーザー名やパスワード、クレジットカード情報、その他の個人情報などの貴重なデータを盗むために使用するウェブサイトにアクセスするよう被害者に奨励しています。

【SMS フィッシング】
ほとんどのフィッシングの試みは電子メールで行われますが、NCSC はテキストメッセージ(SMS)を含む他の方法でフィッシングを実行しようとする試みを観察しています。

従来、SMS フィッシングでは、政府による支払いやリベート(税のリベートなど)などの金銭的なインセンティブをルアーの一部として使用することが多くありました。コロナウイルス関連のフィッシングは、特に流行の経済的影響と政府の雇用と財政支援パッケージに照らして、この金銭的なテーマを

続けています。たとえば、一連の SMS メッセージでは、英国政府をテーマにしたルアーを使用して、電子メール、住所、名前、および銀行情報を収集します。これらの SMS メッセージは、"COVID" および "UKGOV" (図 1 を参照) からのものであると見なされ、フィッシング サイトへの直接リンクが含まれています (図 2 参照)。
この例が示すように、悪意のあるメッセージは電子メール以外の方法で受信される可能性があります。SMS に加えて、可能なチャネルには WhatsApp やその他のメッセージング サービスが含まれます。悪意のあるサイバーアクターは、フィッシングキャンペーンで金融テーマを引き続き使用する可能性が高いです。具体的には、COVID-19 に対応する新しい政府援助パッケージをフィッシングキャンペーンのテーマとして使用する可能性が高い。

【資格情報の盗難に対するフィッシング】
多くのアクターが、ユーザーの資格情報を盗むために COVID-19 関連のフィッシングを使用しています。これらの電子メールには、以前に言及された COVID-19 ソーシャルエンジニアリング技術が含まれ、時にはルアーを強化するために緊急を装う文言が利用されます。

ユーザーがハイパーリンクをクリックすると、パスワード入力フォームを含むスプーフィングされたログイン Web ページが表示されます。これらのスプーフィングされたログインページは、Google や Microsoft が提供するメール サービスや、政府のウェブサイトを通じてアクセスされるサービスなど、幅広いオンライン サービスにを模倣している可能性があります。

受信者をさらに誘惑するために、ウェブサイトには URL 内に COVID-19 関連の文言が含まれていることが多くあります(例えば、「コロナウイルスビジネスアップデート」、「covid19 アドバイザリー」、「cov19esupport」など)。これらのスプーフィングされたページは、正規の、または正確に有名なウェブサイトを偽装するように設計されています。悪意に気付く唯一の方法は、ウェブサイトの URL を調べることです。状況によっては、悪意のあるサイバーアクターは、意図した被害者のためにこれらのなりすましログインウェブページを特別にカスタマイズします。

被害者がスプーフィングされたページにパスワードを入力すると、攻撃者は被害者のオンラインアカウント(電子メールの受信トレイなど)にアクセスできます。このアクセスは、個人情報や機密情報を取得したり、被害者のア

ドレス帳を使用してフィッシングメールをさらに広めるために使用できます。

【マルウェア展開のフィッシング】

多くの脅威アクターは、COVID-19 関連のルアーを使用してマルウェアを展開しています。ほとんどの場合、アクターは、被害者に添付ファイルを開いたり、リンクされた Web サイトから悪意のあるファイルをダウンロードするように誘導する電子メールを作成します。被害者が添付ファイルを開くと、マルウェアが実行され、被害者のデバイスが侵害されます。

たとえば、NCSC は、「エージェント テスラ」のキーロガーのマルウェアを展開するさまざまな電子メール メッセージを観察しています。電子メールは、テドロス・アダノム・ゲブレエソス WHO 事務局長から送られたように見せかけています。このメールキャンペーンは 2020 年 3 月 19 日(木)に始まりました。もう一つの同様のキャンペーンは、流行と戦うために温度計とフェイスマスクを提供しています。電子メールは、これらの医療製品の画像を添付することを目的としているように見せかけて、代わりにエージェントテスラ用のローダーが含まれています。

その他のキャンペーンでは、電子メールには Microsoft Excel の添付ファイル（"8651 8-14-18.xls" など）が含まれているか、またはリンク先ページにリンクしている URL が含まれています。どちらの場合も、Excel ファイルには、有効になっている場合は、埋め込みダイナミック リンク ライブラリ (DLL) を実行して "Get2 ローダー" マルウェアをインストールするマクロが含まれています。Get2 ローダーは、"GraceWire"トロイの木馬をロードして観察されています。

"TrickBot" マルウェアは、さまざまな COVID-19 関連のキャンペーンで使用されています。1 つの例では、COVID-19 に関連する情報を対象とするドキュメントを使用して、電子メールはイタリアのユーザーを対象とします (図 3 を参照)。このドキュメントには、バッチ ファイル (BAT) をダウンロードする悪意のあるマクロが含まれており、JavaScript が起動され、TrickBot バイナリがシステム上で実行されます。

〇免責 事項

このレポートは、CISA、NCSC、および業界の情報源から得られた情報に基づ

いて作成されます。すべてのリスクを回避する意図で行われた調査結果と勧告は提供されておらず、勧告に従ってはそのようなリスクをすべて取り除くわけではありません。情報リスクの所有権は、関連するシステム所有者に常に残ります。

CISA は、分析の対象を含む商用製品またはサービスを推奨しません。サービスマーク、商標、製造業者、またはその他の方法による特定の商用製品、プロセス、またはサービスへの言及は、CISA による支持、推奨、または好意を構成または暗示するものではありません。