

2020 年 8 月 4 日

厚生労働省大臣官房参事官(サイバーセキュリティ・情報システム管理担当)殿

内閣官房内閣サイバーセキュリティセンター 総括参事官

新型コロナウイルスワクチン開発を標的とした 医療、製薬分野へのサイバー攻撃についての対応について

2020 年 7 月、新型コロナウイルスワクチン開発を行う世界の研究機関等に対して、その開発情報の窃取を目的としたサイバー攻撃が盛んになっていることが、英国、米国等の政府から公表されているところです。こうした中、日本時間 8 月 2 日未明、米国 DHS(国土安全保障省)傘下の CISA(サイバーセキュリティ及びインフラストラクチャセキュリティ庁)は、以下のような警告を発信しています。



対応策として、2020 年 5 月 5 日に発出した、米国、英国の 2 国による合同注意喚起が引用されています。サイバー攻撃は国境を超えた手口であり、我が国においても、世界各国と同様、医療、製薬分野等に対するサイバー攻撃が同様に発生しているリスクが高まっていると思われますので、貴省所管の機関、組織等に必要な注意喚起をお願いします。

特に内部部門の独立性が見受けられる研究機関等では、サイバーセキュリティについては一元的な体制を整備し、対策を講じることが肝要です。

■参考資料(仮訳です。解釈は原文が優先されます。)

- 英国と米国の主要医療機関にサイバー警告を発行(2020 年 5 月 5 日 米国 CISA)
- 注意喚起(AA20-126A)APT グループはヘルスケアとそれに必要なサービスを標的にしている(2020 年 5 月 5 日 米国 CISA)

■英国と米国の主要医療機関にサイバー警告を発行

(原題: CYBER WARNING ISSUED FOR KEY HEALTHCARE ORGANIZATIONS IN UK AND USA)

最初のリリース日: 2020 年 5 月 5 日

<https://www.cisa.gov/news/2020/05/05/cyber-warning-issued-key-healthcare-organizations-uk-and-usa>

ワシントン-英国と米国のセキュリティ機関は、コロナウイルス対策に関与する組織を標的とした悪意のあるサイバーキャンペーンが行われていることを公表し、安全のためのヒントを提供します。本日(5月5日)に国際的なヘルスケア及び医療研究機関向けの勧告が公開されましたが、ここでは、合理的に推測できるパスワードを3つのランダムな単語で作成されたパスワードに変更し、2要素認証を実装して侵害の脅威を減らすように助言しています。

英国の国家サイバーセキュリティセンター(NCSC)と米国のサイバーセキュリティ及びインフラストラクチャセキュリティ庁(CISA)は、医療機関及び医学研究組織に対する大規模な「パスワードスプレー」キャンペーンを観察してきました。「高度な持続的脅威」(APT)グループは、国家の優先事項に匹敵する大量の個人情報、知的財産及び情報を収集するため、そのような組織を標的にしています。

NCSC のオペレーションディレクター、ポールチチェスターは次のように述べています。

「私たちは、コロナウイルスの発生中にサイバー攻撃から身を守るため、英国の健康と研究サービスのサポートに全力で注力しています。保健機関からのサポートの要求に優先順位を付け、コロナウイルスへの対応に関与する業界と密接に連絡を取り続けることにより、悪意のある活動を彼らに通知し、彼らを守るために必要な措置を講じることができます。しかし、これを単独で行うことはできません。ヘルスケアの政策立案者と研究者は、パスワードスプレーキャンペーンから身を守るために私たちの実行可能な対策を実施することを推奨します。」

CISA アシスタントディレクターであるブライアンウェアは、次のように述べています。

「CISA は、医療サポートサービスと供給を提供する医療機関と民間組織がインシデントを防止し、COVID-19 への対応に集中できるよう、これらの組織に対するサイバーセキュリティの確保を優先しています。CISA と NCSC 及び業界パートナーとの信頼できる継続的なサイバーセキュリティコラボレーションは、特に医療組織が最大限の能力で作業しているこの時期に、市民や組織を保護する上で重要な役割を果たします。」

治安当局者によれば、コロナウイルスの発生に関連する情報を収集する可能性が高いと思われる国及び国際的な医療機関、製薬会社、研究機関、地方自治体を対象とした攻撃を確認しています。

「パスワードスプレー」は、一般的に知られているパスワードを使用して多数のアカウントにアクセスする試みです。NCSC は以前、攻撃者が個人及び企業のアカウントとネット

ワークへのアクセスを取得するために使用することが知られている、最も一般的にハッキングされたパスワードを明らかにしました。CISA には、組織や個人が自分のパスワードを選択して保護するときによくある間違いをしないようにするためのセキュリティヒントシートがあります。この最新のレポートは、4 月 8 日に NCSC と CISA が発表したサイバー犯罪者が自分自身の利益のためにコロナウイルスの発生を悪用しているとする合同勧告に続くものです。コロナウイルス関連のサイバー攻撃の頻度は、今後数週間から数か月にわたって増加すると予想されます。

先月、NCSC は、コロナウイルス関連の電子メール詐欺の増加を確認したことを踏まえ、疑わしい電子メールレポートサービスを作成しました。最初の 1 週間で、このサービスは 25,000 を超えるレポートを受け取り、395 のフィッシングサイトが停止されました。

■注意喚起 (AA20-126A)

APT グループはヘルスケアとそれに必要なサービスを標的にしている

(原題 : APT Groups Target Healthcare and Essential Services)

最初のリリース日 : 2020 年 5 月 5 日

<https://us-cert.cisa.gov/ncas/alerts/AA20126A>

○概要

米国国土安全保障省 (DHS) のサイバーセキュリティ及びインフラストラクチャセキュリティ庁 (CISA) と英国の国家サイバーセキュリティセンター (NCSC) による合同注意喚起です。CISA と NCSC は、APT グループがサイバー運用の一環として COVID-19 のパンデミックを悪用している兆候を継続的に観測しています。この合同注意喚起は、国内及び国際的な COVID-19 の対応に関与する組織に対する APT グループの継続的な活動に対するものです。これらの攻撃者が組織を標的にするために使用しているいくつかの方法について説明し、対策についての助言を提供します。以前、2020 年 4 月 8 日から悪意あるサイバー攻撃者に悪用されている COVID-19 に関して発出した共同 CISA-NCSC 注意喚起 : (AA20-099A) では、サイバー犯罪者及び APT グループによる COVID-19 パンデミックの悪用について詳述しています。この共同 CISA-NCSC 注意喚起は、COVID-19 に関連する進行中の悪意のあるサイバー活動の最新状況を提供します。CISA と NCSC の COVID-19 合同注意喚起のグラフによる概要については、次のガイドを参照してください。

○COVID-19 関連のターゲティング

APT 攻撃者は、国内及び国際的な COVID-19 の対応に関与する組織を積極的に標的にしています。これらの組織には、医療機関、製薬会社、学界、医学研究機関及び地方自治体が含まれます。APT 攻撃者は、国の優先事項に匹敵する大量の個人情報、知的財産及びインテリジェンスを収集するために、頻繁に組織を標的としています。パンデミックにより、APT 攻撃者が COVID-19 に関連する情報を収集することへの関心が高まった可能性があります。たとえば、攻撃者は国内及び国際的な医療政策に関する情報を入手したり、COVID-19 関連の研究に関する機密データを取得しているようです。

○製薬及び研究機関のターゲティング

CISA と NCSC は現在、脅威攻撃者が製薬会社、医学研究機関及び大学を標的にした多くのインシデントを調査しています。APT グループは、機密性の高い研究データや知的財産を盗んで商業的利益や国家利益を得るために、そのような組織を頻繁に狙っています。COVID-19 関連の研究に関与している組織は、COVID-19 関連の医療に関する国内の研究活動についての情報を求めている APT 攻撃者にとって魅力的な標的です。グローバルな活動

範囲と国際的なサプライチェーンによって、これらの組織は、悪意のあるサイバー攻撃者に晒される機会が増加しています。攻撃者はサプライチェーンをより保護された標的へのアクセスを取得するために利用できる脆弱なリンクと見えています。多くのサプライチェーン要素も、結果として生じたリモートワークやその新しい脆弱性の影響を受けています。最近 CISA と NCSC は、APT 攻撃者が標的企業の外部 Web サイトをスキャンし、パッチが適用されていないソフトウェアの脆弱性を探す活動を観測しました。攻撃者は、Citrix の脆弱性 CVE-2019-19781、Pulse Secure、Fortinet 及び Palo Alto の仮想プライベートネットワーク (VPN) 製品の脆弱性を利用することがわかっています。

○COVID-19 関連のパスワードスプレー活動

CISA と NCSC は、APT グループが実施した大規模なパスワードスプレーキャンペーンを積極的に調査しています。これらの攻撃者は、この種の攻撃を使用して、英国や米国を含む多くの国の医療機関や国際的な医療機関を標的にしています。以前、APT グループはパスワードスプレーを使用して、政府、緊急サービス、法執行機関、学界及び研究機関、金融機関、電気通信及び小売企業を含む、セクター全体のさまざまな組織及び企業を標的にしてきました。

○技術的説明

パスワードスプレーは、ブルートフォース攻撃に一般的に使用されるスタイルです。攻撃者は、次のパスワードを試す前に、多くのアカウントに対して単一の一般的に使用されるパスワードを試します。この手法により、攻撃者はアカウントのロックアウトを迅速または頻繁に回避することで、検出されずに成功することができます。これらの攻撃が成功するのは、特定の大規模なユーザーセットに対して、共通のパスワードを持つユーザーが存在する可能性があるためです。APT グループを含む悪意のあるサイバー攻撃者は、組織の詳細を提供するさまざまなオンラインソースからの名前を照合し、この情報を使用して標的となる機関の可能性のあるアカウントを特定します。次に、攻撃者は識別されたアカウントに、よく使用されるパスワードのリストを「スプレー」します。悪意のあるサイバー攻撃者が1つのアカウントを侵害すると、そのアカウントを使用して、資格情報が再利用される他のアカウントにアクセスします。さらに、攻撃者はネットワークを横断して移動して、追加のデータを盗み、ネットワーク内の他のアカウントに対してさらなる攻撃を実行します。

CISA と NCSC が調査した以前のインシデントでは、悪意のあるサイバー攻撃者がパスワードスプレーを使用して組織の電子メールアカウントを侵害し、次にこれらのアカウントを使用して被害者の組織のグローバルアドレス一覧 (GAL) をダウンロードしました。次に、攻撃者は GAL を使用して、パスワードスプレーでさらにアカウントをスプレーしました。

NCSC はこれまで、頻繁に見つかるパスワードの例を提供してきました。これは、攻撃者がパスワードスプレー攻撃で企業アカウントやネットワークへのアクセスを試みるために使用することが知られています。これらの攻撃では、悪意のあるサイバー攻撃者が、月、季節、及び会社または組織の名前に基づくパスワードを使用することがよくあります。

CISA と NCSC は、大規模なパスワードスプレーキャンペーンに関連する活動の調査を続けています。APT の攻撃者は、パンデミックに関連する追加のインテリジェンス活動に答えようとするため、COVID-19 を引き続き利用します。CISA 及び NCSC は、この増大した活動を考慮して、以下の対策についての助言に従うよう組織に助言します。

○対策

CISA と NCSC は、以前にパスワードスプレーとパスワードポリシーの改善に関する組織向けの情報を公開しています。これを実践することで、この種の攻撃による侵害の可能性を大幅に減らすことができます。

- パスワードスプレー攻撃に関する CISA 警告
- パスワードの選択と保護に関する CISA ガイダンス
- パスワードの補足に関する CISA ガイダンス
- パスワードスプレー攻撃に関する NCSC ガイダンス
- システム所有者のパスワード管理に関する NCSC ガイダンス
- パスワード拒否リストに関する NCSC ガイダンス

CISA の小規模組織向け Cyber Essentials は、経営者に対して、IT プロフェッショナルがその文化の中で機能するよう、セキュリティとその行動を文化として発展するための指針原則を提供します。さらに、英国政府の Cyber Aware キャンペーンは、コロナウイルスのパンデミック時にオンラインで安全を保つ方法について、個人に役立つ助言を提供します。これには、パスワード、アカウント及びデバイスの保護に関する助言が含まれます。

以下の他の多くの対策は、このレポートで詳述されているキャンペーンを防御するのに役立ちます。

- ・ VPN、ネットワークインフラストラクチャデバイス及び作業環境へのリモート接続に使用されているデバイスを最新のソフトウェアパッチと構成に更新する。詳細については、エンタープライズ VPN セキュリティに関する CISA のガイダンス及び仮想プライベートネットワークに関する NCSC ガイダンスを参照してください。
- ・ 多要素認証を使用して、パスワード侵害の影響を軽減する。米国国家サイバーセキュリティ意識向上月間の多要素認証のハウツーガイドをご覧ください。また、多要素認証サービスと 2 要素認証の設定に関する NCSC ガイダンスもご覧ください。
- ・ 重要な運用システムの管理インターフェースを保護する。特に、ブラウズダウンアーキテクチャを使用して、攻撃者が最も重要な資産への特権アクセスを簡単に取得

できないようにする。管理インターフェースの保護に関する NCSC ブログを参照してください。

- ・ セキュリティ監視機能を設定して、ネットワーク侵入の分析に必要なデータを収集する。NCSC のログセキュリティの紹介を参照してください。
- ・ インシデント管理プロセスを確認して更新する。インシデント管理に関する NCSC ガイダンスを参照してください。
- ・ 最新のシステムとソフトウェアを使用する。これらにはより優れたセキュリティが組み込まれています。古いプラットフォームやアプリケーションからすぐに移行できない場合は、ポジションを改善するための短期的な手順があります。旧式のプラットフォームのセキュリティに関する NCSC ガイダンスを参照してください。

このほか、さまざまなシナリオにわたって繰り返されるマルウェアベースの攻撃への防止に投資することを検討します。ランサムウェアと悪意のあるコードからの保護に関する CISA のガイダンスをご覧ください。マルウェア及びランサムウェア攻撃の軽減に関する NCSC ガイダンスを参照してください。