状況認識：
COVID-19 感染拡大に伴い
サイバー脅威が増加―その防御方法は？

24 March 2020 | Adam Meyers（CrowdStrike）

注意：こちらのブログは、COVID-19 関連の攻撃アクティビティに関する最新情報を頻繁に更新しています。是非ご覧ください。

2020 年 3 月 23 日：確認済みアクティビティの最新情報

COVID-19 が世界各地で猛威を振るうなか、政府組織や企業は、従業員や顧客、パートナーの安全と健康を確保すべく、業務遂行の場所とやり方を急速に変化させています。動きのある環境のなか、絶えず変化するパラダイムが組織のセキュリティ体制に重大な影響を及ぼしています。パンデミックの上昇曲線を平坦化することを望む組織のあいだでは、テレワーク、「在宅勤務」が新たな常識になりつつあります。リモートワークを取り入れてすでに数年経過している一部の企業であれば、このような危機に瀕しても、既存のソリューションやポリシーを拡張すればよいだけです。在宅勤務をこれまでにないコンセプトと捉えるその他の企業では、新たな現実に対応するテクノロジー、オペレーション、ポリシーの準備がないために、次のような課題に直面しています。

- パーソナルデバイスや自宅の E メールを使用して業務を行ったり機密情報を扱う
- テレワークをサポートするために、会社の資産のプロビジョニングを行う
- リモートサービス、コーポレート VPN、そのために使用する 2 要素認証を適切に導入および構成する

攻撃者らは、このような課題を敏感に察知し、その状況を自分たちの利益のために利用しようとしています。このブログでは、サイバー脅威の戦略と、2020 年 1 月から本記事の公開時点までに確認された攻撃について、その概要を紹介します。

戦略のハイライト：フィッシング

さまざまな**攻撃者**が、初期アクセスの際の攻撃ベクトルとしてフィッシングを最も多く用いています。フィッシング攻撃では、被害者の欲や恐怖に付け込むケースが多発しています。悪名高い「ナイジェリアの手紙」詐欺は、人間の欲を悪用する攻撃の例です。この手口では、富を持つものが被害者をうまい話で釣ろうとします。COVID-19 の世界的拡大は、広く恐怖をもたらし、世界中の人に注目されています。フィッシング攻撃では、コロナウイルス関連のニュースや公式のガイダンスに関する新情報を持ちかけて、ユーザーをおびき寄せます。

CrowdStrike® Intelligence は、これまでに確認されたケースに加え、今後数か月には、**健康を守るための助言や感染率に関するニュースなどを利用するフィッシング攻撃**が増加するであろうと、確信しています。

健康への興味に訴えるフィッシング攻撃に加え、在宅勤務の従業員が増加したことに目を付ける攻撃者が現れる可能性もあります。そして、関係者になりすまし、企業のガイダンスや手順、人事連絡、IT 上の問題やリソースをネタにしてユーザーをおびき寄せるという方向にシフトするかもしれません。

現在ではまだこのような搾取的な攻撃を直接確認してはいませんが、標的型攻撃においては、ここ数か月の間に、業務や人事に関係するドキュメントでユーザーをおびき寄せるケースが多数発生しています。業務継続のために、従業員がますます E メールに依存することになる今後は、正式なビジネス文書を模倣するフィッシング攻撃が増加すると予想されます。

確認済みのアクティビティ：eCrime(サイバー犯罪)

パンデミックが広がるなか、CrowdStrike は、COVID-19 に便乗する eCrime（サイバー犯罪、特に金銭取得を目的とする）活動の継続的な発生を確認しています。攻撃活動は各国の言語で展開されています。複数の形式の添付ファイルと、さまざまな COVID-19 関連情報が使用されており、この種の攻撃が、これまでも、また今後も広範囲に拡大することが予想されます。COVID-19 に便乗した攻撃活動は、アジアから世界へと拡大するウイルスの軌跡をたどっています。各地の状況に関するニュースが報じられるとともに、攻撃活動のテーマやターゲットが変化しています。たとえば、最近のイタリアの深刻な状況が明らかになると、WIZARD SPIDER が、イタリアの金融機関の顧客を標的に、アカウントの認証情報詐取を目的として、ダイナミック Web インジェクション用のファイルをデプロイしていることが確認されました。

サイバー犯罪者グループ **MUMMY SPIDER** は、2020 年 1 月下旬には、COVID-19 の流行にいち早く反応していました。この攻撃者らは、保健所を騙る日本語のスパムを送信して、Emotet ダウンローダーを配布しました。このダウンローダーは、**WIZARD SPIDER 開発の TrickBot** のダウンロードとインストールを行うよう設計されたものです。

その後も、CrowdStrike Intelligence は、Gozi ISFB、Nemty ランサムウェア、SCULLY SPIDER 開発の DanaBot、GRACEFUL SPIDER 開発の GetAndGo Loader、南米を標的とするマルウェア Kiron などのマルウェアを配布する複数の攻撃を特定しています。また、サイバー犯罪者グループが、**COVID-19 をテーマとしたツールを販売**しようとしていたケースもありました。COVID-19 の感染マップを装ったペイロードプリローダーを用いたフィッシングも確認されています。

確認済みアクティビティ：標的を定めた侵入

COVID-19 の影響が各国に及ぶなか、CrowdStrike Intelligence は、複数の国家主導の攻撃者グループによるスピアフィッシング攻撃が、過去数か月間にわたり継続的に発生していることを確認しました。さらに、これらの攻撃者グループの多くが、COVID-19 に便乗した攻撃を行っていたことも観察されています。2020 年 2 月には、中国ベースの攻撃者グループ PIRATE PANDA による、COVID-19 に関するドキュメントをおとりにした活動が確認されています。北朝鮮の VELVET CHOLLIMA の活動も続行中で、最近では、独自のマルウェア BabyShark を韓国ベースの企業に送り込むために、COVID-19 がテーマのドキュメントを利用していました。

戦略：リモートサービスへの攻撃

企業は、従業員を在宅勤務に切り替え、サポートするために、SaaS やクラウドベースのリモート接続サービスの利用を増やすことが予想されます。リモートワーキングサービスの立ち上げにおいて、セキュリティ上のささいな人的エラーが生じれば、セキュリティリスクが生じる可能性があります。

特に犯罪者らは、ユーザーの SaaS アカウントや組織のデータへのアクセスを目論み、リモートサービスの認証情報を継続的に収集しています。ビッグゲームハンティング（BGH：大物狙い）と呼ばれる大企業を狙うランサムウェア攻撃では、最初の侵入の際に、特にリモートデスクトッププロトコル（RDP）に対するブルートフォー

ス攻撃やパスワードスプレー攻撃が行われています。現在、高度な BGH 攻撃の活動が非常に活発化しています。COVID-19 の影響で発生している人員配置の混乱に付け込もうとするだけでなく、在宅勤務者のデバイスへの侵害も行われるでしょう。

戦術：自動音声を使用したビッシング（Vishing）や技術サポートを装う詐欺

テレワークなどの柔軟な業務体制へと移行すると、業務の遂行・継続のために、従業員は電話による通信により依存するようになります。攻撃者らはこの状況に乗じて、正当な通信を装って悪事を働こうとするでしょう。このような攻撃の形態として、音声によるフィッシングである「ビッシング」や自動音声詐欺、技術サポート詐欺が考えられます。

COVID-19 のアウトブレイクに便乗したビッシングや自動音声による詐欺は、すでに確認されています。当初このような詐欺コールの一部は、米国西海岸をターゲットとしていました。また、運輸や旅行業などの感染の影響を受けた業界も狙われました。ビッシングとスミッシング（SMS を利用するフィッシング）を組み合わせて詐欺を実行したり、モバイルデバイス上に悪質なコンテンツをロードさせたりというケースも発生しています。

技術サポート詐欺では、通話、ポップアップによる警告、リダイレクトなど、さまざまな拡散方法が用いられています。これらの詐欺のテーマは、直接 COVID-19 とは関係ない場合がありますが、短い間に在宅勤務に移行しなければならないオフィスワーカーの増加により、リモートコンピューティングに不慣れであったり、自分で問題を解決できないユーザーをターゲットとした、技術サポート詐欺のリスクは高まるでしょう。

COVID-19 に便乗した詐欺に対抗するための推奨事項

COVID-19 の世界的な拡大に伴い、CrowdStrike は、悪質なサイバー犯罪者らが、今後もこの状況に乗じた攻撃を仕掛けてくるであろうと予想しています。そのため、新しい事業継続計画へと移行する際に直面する可能性のあるサイバー脅威について、企業側と従業員が常に頭においておくこと、また、潜在的なリスクを低減するための緊急措置について通知を受けることが不可欠です。

CrowdStrike は、リモートサービス、VPN および多要素認証ソリューションへのパッチ適用を確実に実施し、適切な統合を行うこと、また、在宅勤務の従業員にセキュリティ意識向上のためのトレーニングを実施することにより、強力な防衛体制を整えることを推奨しています。

このような想定外の展開に対処できるように、CrowdStrike は、製品をご利用中のお客様に向け、**期間限定の新プログラムを 2 つ**提供しています。これらのプログラムは、新しい在宅ワーカーが使用する多数の管理対象 / 非対象のデバイスによってもたらされる問題に対処するものです。

確認されたアクティビティの最新情報：3 月 23 日 月曜日

CrowdStrike Intelligence は、以下のアクティビティを新たに確認しました。

- 2020 年 3 月 23 日、ヨーロッパを拠点とする複数の病院が、Netwalker ランサムウェア（別名 KazKavKovKiz、Mailto、Mailto2、KoKo）による被害に遭ったことが公表されました。2020 年 3 月 22 日に始まったとされるこのインシデントは、COVID-19 に便乗した攻撃によるものです。
- 2020 年 3 月をとおして、情報詐取を行うトロイの木馬 RedLine が COVID-19 に乗じたスパム攻撃で使用されました。このスパムは、病気の潜在的な治療法をシミュレートして、その有効性を評価する団体を偽って送信されていました。
- ダイナミック Web インジェクションを行うマルウェア TrickBot が、イタリア拠点の金融機関の顧客に配信されました。これは、WIZARD SPIDER による COVID-19 便乗型攻撃の一環である可能性が高いと考えられます。このダイナミック Web インジェクション攻撃は、現在ロックダウンが行われているイタリアでオンラインバンキングの必要性が増していることを悪用するものと思われます。
- 2020 年 3 月 16 日、オーストラリアのサイバーセキュリティセンター（ACSC）は、地域の COVID-19 テスト施設に関する情報提供を謳うテキストベースのフィッシング詐欺の発生を**報告**しました。テキスト内の URL を開くと、悪質な Android アプリケーションパッケージを経由して、コモディティ型のバンキング系トロイの木馬がドロップされます。
- 2020 年 3 月 18 日には、政府機関を標的とした Nemty ランサムウェア（v2.6）のサンプルが検出されました。医療機関の最高経営責任者を装い送信された E メールは、パンデミックについて話し合う年次会合を案内するものでした。
- 2020 年 3 月 18 日、TWISTED SPIDER は、パンデミックの状況が落ち着くまでの間、医療機関への攻撃を控えることを発表しました。他の攻撃者グループも、医療業界への攻撃を自粛すると発表しています。
- CrowdStrike Intelligence は、MUSTANG PANDA による、COVID-19 便乗型攻撃が 2020 年 2 月末から継続中であることを確認しています。それらのインシデントでは、悪質なショートカットファイル（LNK）を使用して、中国語、英語、ベトナム語で書かれた「おとり」のドキュメントを拡散していました。
- CrowdStrike Intelligence は、過去 1 週間のハクティビストの活動状況から判断して、特にラテンアメリカとヨーロッパにおいて、COVID-19 感染拡大期間にハクティビズムが急増すると予測しています。過去 1 年間を見ても、ラテンアメリカのハクティビズムの割合は、これまでよりすでに増加していました。これは主に同国の多くの地域に生じている政情不安によるものと考えられます。ウイルス拡大緩和のために、大規模なデモや集会がますます禁止されるようになり、抗議の選択肢が狭まることから、このような攻撃活動の増加が見込まれます。

追加のリソース

- COVID-19 時代のサイバーセキュリティへの対応に関して、**CrowdStrike の CEO、George Kurtz** がブログで発信しています。
- COVID-19 蔓延時におけるサイバーセキュリティ上の課題や、テレワーカーの安全のための推奨事項に関する詳細については、**CrowdStrike の CTO、Mike Sentonas** および**チーフプロダクト・エンジニアリング・オフィサーの Amol Kulkarni** のブログをご覧ください。
- **CrowdStrike COVID-19 リソース Web ページ**をご覧になり、御社とリモートワーカーのセキュリティ確保に役立つ情報を入手してください。
- CrowdStrike Intelligence とエンドポイントセキュリティエキスパートによるオンデマンドの Web キャストをご覧ください。**『Cybersecurity in the Time of COVID-19（新型コロナウイルス蔓延時代のサイバーセキュリティ）』**
- **CrowdStrike の 2020 年グローバル脅威レポート**をダウンロードできます。