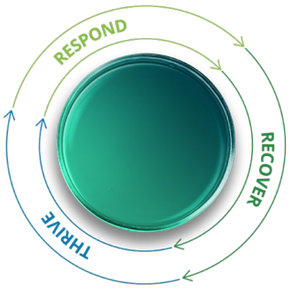
Issue 7| May 20, 2020

Deloitte.



COVID-19 Global Cyber Risks: Attack surfaces expand amid return to work efforts 日常を取り戻していく中で攻撃対象領域は拡大します

Deloitte Cyber Threat Intelligence (CTI) が明らかにした、最新のサイバー脅威とその動向に焦点を当て、世界的な流行であるCOVID-19 パンデミックに対応、回復、成長するためのサイバーリスク管理について短期的な提言をま

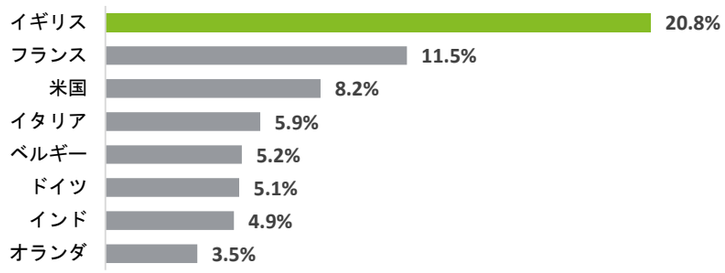
アジャイルな攻撃者はあらゆる業界や地域をターゲットにしています。

ここ数週間で、7か国が COVID-19 によるロックダウンを緩和し始めました。しかし、オンサイトワークとリモートワークの両方を可能にするハイブリッドワーク環境への移行が遅々として進まない中で、パンデミック関連のサイバー脅威は減少していないように見えます[1]。コロナウイルスをテーマにしたサイバー攻撃は、今や世界各国で確認されており、1月は対前年比17%、2月は同52%、3月は同131%とウイルスは急増しています[2]。

今週のブリーフィングにもあるように、標的型攻撃も増加しており、人気のアプリケーションやプラットフォームだけでなく、あらゆる業界全体が対象となる中で、週を追うごとにセキュリティ警戒強化や従業員教育、サイバーリスクを意識したカルチャーの必要性が明確化しています。

悪意あるコロナウイルススパムに標的にされている国

件名に「コロナウイルス」が含まれた悪質スパムメールが送られた配信上位国とシェア



* 2020年1月1日~3月27日

出典: Trend Micro、https://www.statista.com/chart/21291/countries-targeted-most-by-malicious-coronavirus-spam/

[1] 出典:https://www.businessinsider.com/microsoft-research-shows-coronavirus-cyberattacks-in-every-country-2020-4
[2] 出典:https://www.fortinet.com/blog/threat-research/preparing-for-the-surge-in-attacks-targeting-remote-workers.html

注意: 攻撃者は機を狙って、なりすましています。COVID時代には誰しもが標的になり得るのです。

医療機器メーカーへの標的型攻撃

影響範囲 ： 医療、ヘルスケア|地域:グローバル

Fortinetは2020年5月1日、医療機器メーカーを狙ったスピアフィッシング攻撃（特定のターゲットに対するフィッシング詐欺）が開始されたと報じました。「医薬品に関する問い合わせ」という件名のスパムメールは、COVID-19向け医薬品や機器に関する情報を求める内容になっています。メールには「Medical Inquiry - L.A.B. Equipment.doc」という悪意あるファイル添付がされており、この添付ファイルを開くと、受信者のシステムにリモートキーロガーがインストールされるというものです。

米国の中小企業を標的とした攻撃

影響範囲 ： 全ての分野|地域:米国

2020年5月8日、COVID-19 救済金を必要としている米国の中小企業を標的にした悪意あるスパムキャンペーンが行われました。米国政府を装ったスパムメールで、一見正規のメールアドレスから送信されているように見えますが、実際には企業ドメインから送信されています。メールには、受信者の署名を要求する添付ファイルが含まれていましたが、実際には、ハッカーがWindowsコンピューターを制御および監視できる悪意あるファイルでした。

韓国企業に対する標的型攻撃

影響範囲 ： 製造業|地域:韓国

2020年5月8日に米国の中小企業向けに行われたスパムキャンペーンの一環として、韓国の製造業も標的になりました。韓国のケースは、米疾病予防管理センター (the Centers for Disease Control and Prevention：CDC)を装い、悪意ある添付ファイルが含まれたスパムメールが送られるというものでした。ファイルが開かれると、ハッカーは受信者のシステムにバックドアで侵入し、悪意あるコマンドの実行や、感染させたコンピューター上のキーストロークのログ、認証情報の取得を可能とします。

米国の会計士を標的とした攻撃

影響範囲 ： プロフェッショナルサービス|地域:米国

2020年5月8日に行われた悪質なスパムキャンペーンに関連する3つ目のメールは、米国の会計士に送信されました。COVID-19 関連の最新情報が含まれた米国公認会計士協会（AICPA）の会員向けメールで、受信者が添付ファイルを開くと、リモートアクセス用のトロイの木馬が作動し、ハッカーがユーザー情報を盗み出し、バックドアのコマンドを実行できるようにするというものです。

攻撃のターゲットは人気のコラボレーションプラットフォーム

影響範囲:全ての分野|地域:グローバル

Deloitte CTIは2020年5月6日から12日までの1週間、リモートワークの従業員をサポートする人気コラボレーションプラットフォームを標的とした一連の新しいフィッシングキャンペーンを観測しました。ある事例では、偽の証明書のエラー通知を使ってユーザーを騙し、Cisco Webexの企業認証情報を共有させていました。またこれに関連したものでは、OutlookとOffice 365用に偽のログインページが作成され、気付かず偽のサイトにログインすると、サイバー犯罪者がユーザーの認証情報を盗むことができたという事例もあります。トレンドマイクロは、2020年1月から4月27日の間だけで、この種のフィッシング詐欺を約5万件検出しています。

サイバーインシデントを未然に防ぐための対策

1. メールを開く前に、別の通信手段や安全な媒体を使って、メールの送信者を確認してください。メッセージに記載されている連絡先情報を使用せず、添付ファイルのクリックや、リンクへのアクセスは行わないようにしましょう。
2. メール・セキュリティ・ゲートウェイに、悪意ある添付ファイルやURLのスキャン、ブロック機能等、高度なセキュリティ機能が備わっているか確認しましょう。
3. フィッシング事例を報告、疑わしいアクティビティにフラグ付けができる高度なメール保護ツールをインストールしましょう。
4. ホスト及びユーザーの動きを追跡し、行動ベース分析に十分なデータを取得しましょう。これにより、疑わしい原因や、ホストやユーザーアカウントを危険にさらす試みの特定に役立てることができます。
5. ヘルプデスク担当者が従業員の身元を確認する方法を定義しましょう。これにより、パスワードのリセットやアカウントの乗っ取りを目的としたソーシャルエンジニアリングのリスクを軽減することができます。
6. グループポリシーにより、Microsoft Officeのアプリケーションでマクロを有効にするユーザーをブロックしましょう。
7. モバイルデバイスのセキュリティプロトコルを強化しましょう。

事例:

COVID-19 の拡散状況が追跡できると主張する悪質なAndroidアプリで、ランサムウェアに感染した事例があります[3]。アプリは人々の動きを追跡するので、COVID-19に発症した際の症状や、検査で陽性反応が出た場合に、保健機関や接触者全員に警告することができます。

現在多くの国 (シンガポール、オーストラリア、イギリスを含む)が、通常稼働を見越して、スマートフォンに接触者追跡アプリをインストールするよう呼びかけていることから、このような例は特に顕著な脅威と言えるでしょう。

アプリ自体がプライバシー問題を提起されていますが、「偽」アプリはさらに大きな被害をもたらす可能性があるため、ダウンロードする前に十分に警戒を強めましょう。

[3] 出典:https://www.bbc.com/news/technology-52319093

回復と成長: COVID-19 によりサイバーリスクを意識した企業文化の必要性が高まり

COVID-19に関連したサイバー脅威が後を絶たない中、企業はセキュリティ技術やポリシーだけでなく、それ以上のものを強化しなければならないということに気づき始めています。また、サイバーリスク管理プログラムを強化する組織文化も醸成しなければなりません。文化醸成の上で"ピープルコンポーネント"（人々という要素）を無視すれば、従業員が問題の一部となり、脅威者が悪意ある行動を起こす引き金となる可能性があります。このことはサイバーリスクカルチャー醸成の必要性をさらに強調しています。以下に基本原則をいくつか示します。

トップから示しましょう。リーダーは組織にとって模範であり、サイバーリスク管理の期待値を設定するのはリーダーの役目です。サイバーリスク認識の優先度を示すために、リーダーは、 COVID-19 に関連する新たな脅威の動向や、ビジネス領域に関連するサイバーリスクの指標を正確に把握、監視し、サイバーリスクをシニアリーダーまで引き上げるべきです。

トレーニングを続けましょう。入社時以降正式なサイバートレーニングを受講していない従業員は、再受講が必要だと考えられます。今こそ、リモートチャネルやモバイルデバイスを活用してトレーニングモジュールを公開しましょう。まだ実施していない場合は、マイクロトレーニングモジュールやゲームアプリを作成し、トレーニングをより身近に、より記憶に残るものにすることを検討してください。

コミュニケーションを図りましょう。サイバーリスクカルチャー醸成のために、リーダー、人事部、およびその他の社内関係者から定期的にコミュニケーションを図り、サイバーリスクの問題に対処し、セキュリティポリシーやプロトコルについて従業員に注意喚起を行いましょう。またメール、テキストメッセージ、ビデオ、その他コラボレーションプラットフォームなど、複数のチャネルを通じてコミュニケーションを図りましょう。

ビジョンを見直しましょう。COVID-19の緊張が続く中で、サイバーリスクを意識した企業文化のビジョンへ見直す時期に来ているのかもしれません。

新たな行動規範はありますか?サイバーリスクを意識したプラクティスを改善する必要はありますか？従業員は今、どのようなサイバーリスクアクションを取るべきでしょうか(例：COVID-19に関連するメールを受信した際の懐疑心の高まり、業務を遂行する際のサイバーリスクへの配慮の強化、認識されるリスクの増加等 ...)？

望ましい行動には報酬を与えましょう。組織の優先事項には、そのタレントライフサイクル、つまり、従業員の採用、昇進、育成、および評価が反映されています。サイバーリスクカルチャーを醸成するためには、サイバーリスクに対する行動を評価管理プロセスにリンクさせること、ビジネスユニットごとにサイバーリスクメトリクスを公表すること、さらには脅威のベクトルをクラウドソーシングすることも検討すべきです。

Deloitteはクライアントに寄り添い、COVID-19を乗り越えるサポートをします

関連情報:

- **COVID-19 :デジタルビジネスで未来を形作る**
- **信頼をCOVID-19 リカバリーに組み込み**
- **COVID-19 経済事例:ビジネスリーダーのシナリオ**

Deloitte Cyberはダイナミックで接続された世界の進歩を促し、複雑な問題を解決して自信に満ちた未来を築きます。人間の洞察力、技術革新、包括的なサイバーソリューションを駆使して、あらゆる場所でサイバーを管理することで、社会、そしてあなたの組織がどこにいても成長できるように貢献します。


Emily Mossburg
Global Cyber Leader
+1 571 766 7048
emossburg@deloitte.com


Amir Belkhelladi
Canada
+1 514 3937035
abelkhelladi@deloitte.ca


Simon Owen
North South Europe
+44 20 7303 5133
sxowen@deloitte.co.uk


Deborah Golden
US
+1 571 882 5106
debgolden@deloitte.com


James Nunn-Price
Asia Pacific
+61 293227971
jamesnunnprice@deloitte.com.au


Peter Wirnsperger
Central Europe
+49 40320804675
pwirnsperger@Deloitte.de


Nicola Esposito
Spain
+34 918232431
niesposito@deloitte.es

For more information contact visit Deloitte.com/covid or Deloitte.com/cyber（日本語）Deloitte.com/jp/cyber

Deloitte Cyberグローバルの翻訳になります。