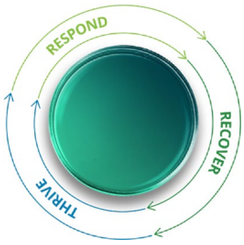
Issue:8|June 3, 2020

COVID-19 Global Cyber risks: Is a major cyberattack looming? 迫り来る大規模サイバー攻撃



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とめました。

COVID-19 は破壊的なサイバー攻撃の基礎を築きます。あなたの組織は準備ができていますか?


HEADLINES TODAY

292,188 views | May 14, 2020, 09:00am EDT

Why The Largest Cyberattack In History Could Happen Within Six Months[1]

パンデミックが招く「史上最大のサイバー攻撃」の危機

[1]出典:https://www.forbes.com/sites/stephenmcbride1/2020/05/14/why-the-largest-cyberattack-in-history-will-happen-within-six-months/#31da7160577c

Deloitte CTIは数週間にわたり、COVID-19 に関連する広範なサイバー攻撃を追跡してきました。一貫して報告されているように、パンデミックは、脅威者の戦術、テクニック、手順が目に見える変化をもたらしていないと確信していますが、組織がさらされているリスクのレベルは変化しています。リモートワークに対応するための大規模スクランブルにより、攻撃対象はかつてないほどに拡大し、**大規模なサイバー攻撃が発生する可能性を高めています。**混沌とした変化の中だからこそ、攻撃者は優位に立とうとしているのです。サイバーセキュリティ態勢を強化していない組織は、まさに今、自社を標的とした脅威や、サードパーティ及びその先の企業を介して自社を知らず知らずのうちに標的にしている脅威に対して効果的に保護、検出、対応する準備ができていないことに気付くかもしれません。

COVID-19特有のサイバー攻撃が増加の一途をたどっています

偽のコンタクトトレーシングアプリがランサムウェアを配信

影響範囲:全ての分野　地域:欧州

2020年5月27日、Deloitte CTIは、悪意あるCOVID-19関連のコンタクトトレーシングアプリを使って、ライフサイエンス、ヘルスケア業界、学会を標的としたランサムウェアの配信を観測しました。セキュリティベンダーのDottor Marc氏は、イタリア全土の薬局、医師、医療機関、大学を標的とした“Unicorn” と呼ばれる新たなランサムウェアについて報告しています。ユーザーは、ソーシャルエンジニアリングにより、悪意あるCOVID-19のコンタクトトレースアプリをダウンロードするよう誘導され、暗号化プロセスが完了すると、感染したデバイスの画面に、イタリア語で300ユーロの身代金を要求する文章が表示されるというものです。

増加傾向にあるモバイルマルウェアの脅威

影響範囲:全ての分野　地域:グローバル

モバイルマルウェアは在宅勤務を続ける従業員をターゲットにしています。研究者らは、COVID-19を利用して連絡先リストへのアクセス、被害者のデバイスからSMSデータを読み取ることができる4つの異なるバージョンのAndroidマルウェアを特定しました。ユーザーは、自身のデバイスとアカウント、特にAndroidデバイスのアプリケーション経由でアクセスされたアカウントを継続的に監視し、認識されないアクティビティやアプリケーションの異常な動作が起きた場合は速やかに報告する必要があります。モバイルアプリ、プラグイン、コーデックをインストールする際には、Google Play StoreやAppleストア、そして必要に応じて企業ポータルといった信頼できるソースから提供されていることを確認してください。モバイルデバイス管理（ MDM ）またはエンタープライズモビリティ管理（ EMM ）ソフトウェアソリューションを導入して、スマートフォンやタブレットを含む企業のモバイルデバイスのセキュリティを強化しましょう。

フィッシング攻撃がビジネスインテリジェンスに及ぼす影響

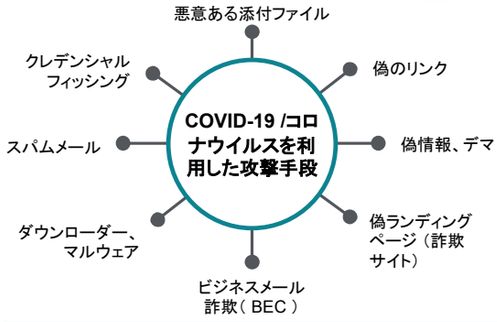
影響範囲:全ての分野　地域:欧州

2020年5月27日、Deloitte CTIは、欧州を拠点とする脅威アクターVendettaが、個人を標的にし、業務上の機密情報を盗むために、COVID-19をテーマにした警察の捜査情報や検出通知を利用したフィッシングメールを観測しました。マクロを使用していない環境であれば、Microsoft Officeドキュメントに埋め込まれたマクロをブロックするか、有効性が確認された署名付きマクロのみを許可して実行する必要があります。疑わしいメールを受信した際は、安全なチャネルを介して別の通信方法で見かけ上の送信者を確認するなど、メッセージ内で提供された連絡先情報を使用しないようにしてください。

ビジネスメール詐欺(BEC)に狙われる救済基金

影響範囲:すべて　地域:米国

Deloitte CTIは、COVID-19を利用したビジネスメール詐欺（ BEC ）攻撃を行っている脅威アクターが、CARES法や米国の失業システムから拠出される資金を狙っていることを観察しました。一例として、ナイジェリアの脅威アクターグループScattered Canaryは、Gmailのドットアカウント機能を悪用し、何百もの偽アカウントを作成、内国歳入庁（ IRS ）や州の失業者向けウェブサイトを利用し、COVID-19コロナウイルスに関連する詐欺請求を行いました。件名に COVID-19に関する情報が含まれている電子メールメッセージに埋め込まれた添付ファイルやリンクは、クリックしないよう従業員に警告してください。



永続的なレジリエンスに関する備忘録

- COVID-19に関連したインシデントを個々に見ると、不安にはなりますが決して予想外の出来事ではありません。しかし、全体で見ると、社会の弱点を狙った攻撃のパターンが見えてきます。これは、あらゆる国や経済のあらゆる分野の組織のサイバーインテグリティを脅かすものです。
- 思い出す度に戦慄が走りますが、2017年のNotPetya攻撃はウクライナから始まったものの、数秒で意図したターゲットを超えて拡散し、最終的にはロシアやデンマーク、英国、米国に至るまでの組織に影響を与えました。
- サイバー攻撃は無数のデバイスを危険にさらし、息を呑むような速さで世界中のネットワークに広がり、そしてサーバーやエンドポイントを操作不能にするのです。
- もし企業システムがCOVID-19 の流行以前にすでにリスクにさらされていたとしたら、まさに今、世界中におけるかなりの割合の人々が企業ネットワークに接続し、脆弱で、セキュアでない不安定なシステム上で機密情報を共有していることになります。企業が直面している脅威を想像してみてください。
- **こうした現状を踏まえ、基本的にサイバーリスク管理プログラムが健全な組織であっても、コロナ後の運用や組織をサポートするための新たなアプローチが必要となる可能性があることから、サイバーへの即応性、対応性、復旧性を再検討し、改善を図る必要があります。**

回復と成長: どこからでも働くことができる環境にするためには、サイバーが必要です

企業規模の破壊的なサイバー攻撃への扉が開かれています。アタックサーフェイス（攻撃対象領域）が急激に拡大するCOVID-19時代において、脅威アクターは、運用システムからバックアップサーバに至るまで、非常に高度かつ洗練された方法で組織の弱点を突いてくることが多くなっています。これらのリスクを軽減するために、組織は新たな教育ツール、技術的ソリューション、およびビジネス戦略を採用しなければなりません。ここでは、いくつかの方法をご紹介します。

インシデント対応計画の見直しと改訂

サイバーインシデント対応プロセスがCOVID-19 の危機管理チームとどのように連携するかを定義する、シンクロナイズされたサイバーインシデント対応計画を作成します。

セグメント分割とゾーニング

フラットなネットワークでは、攻撃者はさまざまなシステムを容易に操作することができます。攻撃の影響を最小限に抑えるために、セグメント分割とゾーニングを改善し、攻撃者の横移動を防ぎましょう。

アクセス管理を強化

効果的なアイデンティティーおよびアクセス管理（ IAM ）セキュリティフレームワークは、識別、認証、許可、アクセスガバナンス、およびアカウンタビリティと5つの主要ドメインのスタンスを向上させる必要があります。リモートワークへのシフトが進む中、組織はセキュリティ優先のクラウド戦略を採用し、特権アクセス管理を強化する必要があります。

IT資産管理の強化

リモートワークへの移行が急速に進んだことで、新たな（おそらくテストされていない）アプリケーション、オペレーティングシステム、デバイスが導入されています。アタックサーフェイス（攻撃対象領域）を限定するためには、分散している資産を監査し、一元管理する必要があります。これには、従業員が現在使用している個人用デバイスも含まれ、ある程度のセキュリティ管理が必要となります。知らないことを保護することはできないのです。

サイバー衛生の改善

サイバー環境の脆弱性は、企業のセキュリティに直接影響を与えます。全てのソフトウェアにパッチを適用し、全てのシステムが適切に構成されていることを確認します。そして全てのセキュリティツールを導入し、効果的なアセットの検出および追跡プロセスを採用することが重要です。

バックアップを合理化

従来のリカバリでは、重要なシステムのデータの冗長化が積極的に行われる傾向にあります。マルウェアに侵入されると、このバックアップ環境によって攻撃の拡散が加速されます。この問題に対処するには、バックアップデータやその他の重要なマテリアルを格納するための保管庫と、保管庫から環境を再構築できる合理化されたデータリカバリゾーンのセットアップを検討してください。

経営幹部は、ビジネスリーダーとCISO（最高セキュリティ責任者）との効果的な会話を促進するために以下の質問を行うと良いでしょう

- サイバーセキュリティに関する役割と責任が明確に定義され、CEOや取締役会に至るまで、組織のあらゆるレベルに周知されていますか？
- ビジネスリーダーは、組織の最も価値のある資産が何であるか、また、どの程度のサイバーリスクを許容できるかということを理解していますか?
- テクノロジーソリューションは、セキュリティとプライバシーを考慮して設計、統合、運用されていますか？
- 事業者は、投資先の事業や製品に対して、設計による安全性の確保と規定の方法を奨励していますか？
- サードパーティ、さらにはその先の企業のサイバーリスクがベンダーとの契約や修復プロセスに組み込まれていますか?

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 の教訓を反映した危機管理戦略を更新
- 職場の再開:レジリエンスの高いリーダーガイド
- Deloitte Insights:世界的な消費回復への道を確立する
- COVID-19 :Next Normal（新しい世界）でのプライバシーとセキュリティ

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

詳細は、（英語）Deloitte.com/covidorDeloitte.com/cyber（日本語）Deloitte.com/jp/cyber

Deloitte Cyberグローバルの翻訳になります。