MANDIANT
NOW PART OF Google Cloud

サイバー・スナップショット・レポート 第3号

『防御側の優位性 - サイバー・スナップショット』レポートでは、サイバー攻撃の最前線でMandiantが得た観察事項と現実世界での豊富な経験に基づき、新たに重要性が増しているサイバー防御のトピックに関する知見をお届けします。今号では以下のトピックを取り上げます。

› パスワードレス認証への道筋 3

› サイバー保険に加入する際のリスクを最小限にするには 7

› セキュリティ・アナリストのケーススタディ：ソフトウェア・サプライチェーン侵害を見つけ出して阻止する 12

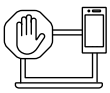
› CISAのCross-Sector Cybersecurity Performance Goals（全業種サイバー・セキュリティ・パフォーマンス目標）でサイバー防御を活性化する 16

パスワードレス認証への道筋

歴史的に、単一パスワードを使用するチャレンジ・レスポンス認証は、本人確認を行う認証手段として組織が活用する主要なメカニズムの1つでした。けれども、付加的な本人確認を行わずに、単一トランザクションで認証するというこのモデルでは、組織に大きなリスクをもたらす可能性があります。

個人情報侵害のために攻撃者が使用する戦術が洗練度を増すにつれて、リスクを軽減するための新しいセキュリティ対策機能や方法が導入されるようになりました。多くの組織が採用している最も一般的なセキュリティ対策機能は、多要素認証（MFA）です。これは、2つ以上の独立した方法を組み合わせて本人確認を行うものです。

Mandiantが多くのインシデントレスポンス調査を通じて観察したところによると、組織は従来のMFA手法の採用を増していますが、一方で、攻撃者は次のような手法を使って、個人情報を侵害する高度な戦術を展開していることがわかりました。



強制的MFAの回避

弱点のあるMFA手法（SMS、プッシュ通知、電話など）の悪用

攻撃者がコントロールするMFA検証・認証用デバイスの導入

このような脅威の拡大により、MFA導入を拡大するための焦点は、番号照合、コンテキスト対応テレメトリー通知、タイムベースドワンタイムパスワード（TOTP）の入力など、より強力なMFA手法を用いる新しいツールにシフトしています。さらに、ベンダーや組織は、Fast Identity Online 2（FIDO2）キー/トークン、ソフトウェア/ハードウェアOpen Authentication（OATH）トークン、または証明書ベースの認証のいずれかを活用することによって、MFA方式をさらに強化しています。

オーセンティケーター

認証の安全性をさらに高めるために、組織の個人識別管理とアクセス管理の一環として統合された「オーセンティケーター」という概念が登場しています。オーセンティケーターは、パスワードという単一のコンテキストから脱却し、複数のコンポーネントを用いて本人確認を行います。オーセンティケーターの例としては、ユーザー名/パスワードに、強力なMFA方式、証明書、デバイス状態コンテキスト、個人識別リスク計算、パスワードレス方式などを組み合わせたマルチコンテキストを挙げることができます。

「オーセンティケーター」という概念を用いることにより、認証の防御線としてパスワードの特異性だけに依存することがなくなり、パスワードが侵害された場合のリスクが全体として大幅に減少します。

パスワードレスとは？

強力なMFA方式をベースにしたパスワードレス認証は、多くの組織で「オーセンティケーター」の一部として導入され始めています。パスワードレスとは、本質的に、知識ベースの秘密情報を必要としない本人確認の方法です。知識ベースの情報の代わりに、所持品（デバイス）または本人の身体（生体認証）を使用して本人確認を行います。パスワードレスを前提に、所有物や本人の身体に基づく要素を要求することで、「知っている情報」（パスワード）を認証の方程式に組み込む必要がなくなり、セキュリティが向上します。

パスワードレス認証を活用する実用的でスケーラブルな方法としては、以下のようなものが考えられます。

- **モバイル認証アプリケーション** – ワンタイム・パスコード（OTP）（同期アルゴリズムに基づく）を生成するか、またはユーザーに表示される数字列を承認や一致に使用することができます。
- **FIDO2ハードウェア・トークン/キー** – 物理的接続、Bluetooth、または近距離無線通信（NFC）のいずれかを使用してデバイスとのインターフェイスが可能になります。FIDO2 WebAuthn方式では、具体的には、デバイスにバインドされたハードウェア・トークンを使用して宛先アプリケーションを認証することができ、この際に、固有の暗号キーペア（ローミング認証デバイスに保存される）を使用し、公開鍵暗号を用いて交換されます。FIDO2 Webauthnは、パスワードレス認証を活用して、フィッシングやなりすまし、中間者攻撃（AitM攻撃）に対抗するための有効な手段です。
- **パスキー** – FIDO2トークンのように動作し、暗号キーペアを生成してモバイル・デバイスにローカルに保存し、公開鍵暗号を使用して、認証対象であるアプリケーション（公開鍵を保持する）と交換します。設定されたパスキーにアクセスするには、モバイル・デバイスに、生体認証または一般的なモバイル・デバイスに共通するPIN/スワイプパターンのいずれかが必要となります。
- **デジタル証明書** – 公開鍵と秘密鍵のペアを使用して、認証要求に応答することにより、有効なデジタル「本人確認」署名を生成できます。最近のデバイスでは、トラステッド・プラットフォーム・モジュール（TPM）を内部認証装置として使用し、秘密暗号鍵を保存することができます。この秘密暗号鍵は、対応する公開鍵を使って「パスワードレス」認証のために検証される証明書への署名に使用します。

- **生体認証** – 人間の固有の身体的特徴を利用して本人確認を行うことができます。生体認証には、多くのスマートフォンやモバイル機器、最新のノートパソコンに搭載されている指紋認証（Touch ID、Fingerprint Unlockなど）や顔認証（Face ID、Face Unlockなど）があります。

オーセンティケーターとしてのパスワードレスを計画する

オーセンティケーターの概念を活用しようとする組織にとって、強化された認証方法をサポートするのが難しいレガシーのアプリケーションやインフラが足かせとなる可能性があります。現在では、個々のアプリケーションごとにオーセンティケーターを組み込むのではなく、サードパーティのシングル・サインオン（SSO）ソリューションを認証のフロントドアとして活用し、認証されたアクセスをバックエンド・アプリケーションに仲介することが一般的となっています。

パスワードレスをオーセンティケーター方程式の一部として計画するには、時間がかかります。高レベルの検討事項には次のようなものが挙げられます。

特定すべきこと

- 認証用IDストレージおよびプラットフォーム（IdP）として機能する、現時点の技術およびプラットフォーム。
- 既存のIDストレージは、パスワードレス認証方式をネイティブにサポートしているが、サードパーティの統合やブローカーが必要になる。
- 組織内に存在する本人確認情報（パスワードレス体験をテスト・検証できる本人確認情報タイプを含む）。
- パスワードレスまたは強力な認証方法をサポートしない本人確認情報タイプ（例：プログラムやサービスアカウント）に対する対策機能や検知強化を補完する。
- パスワードレス統合をサポートしない可能性のあるゲスト/サードパーティユーザーへの影響。
- ユーザーが認証やアクセスに現在利用しているデバイスは何か、またこれらのデバイスがパスワードレス方式をサポートしているかどうかを確認する。
- パスワードレス用に直接統合できるアプリケーション、またはパスワードレス方式をサポートするサードパーティ・プラットフォームとのSSO統合をサポートするアプリケーション。

以下の計画を立てる

- パスワードレス認証に対応するデバイスを調達し、安全に納品・搭載すること。
- パスワードレス体験をユーザーに知ってもらうためのトレーニング・カリキュラム。
- パスワードレス統合を搭載するためのIDストレージとデバイスの設定変更。
- パイロット・ユーザーと候補アプリケーションでパスワードレス統合のテストと検証を行う。
- 初期導入とオンボーディングを行い、パスワードレスの範囲を組織全体に拡大する。

パスワードレスでもう1つ、考慮しておくべき重要な点は、デバイスや鍵の紛失・盗難時の復旧手順を揃えておくことです。これらは現在、本人確認の認証プロセスの中核をなす要素となっているからです。安全な復旧手順を計画するには、組織のリスクだけでなく、ユーザーの登録とセルフサービス体験全体に対する長所と短所を考慮する必要があります。

内部認証装置（TPM内蔵デバイスなど）は、デバイス間で秘密鍵をエクスポート（保存）または同期する機能を提供できますが、鍵が適切に保護され保存されていない場合、これがリスクをもたらす可能性もあります。サードパーティの認証プロバイダーを使用する場合、新しいデバイスで再構成するためのパスワードレスIDを回復する方法として、回復キーとフレーズを考慮することもできます。ローミング・オーセンティケーターがパスワードレス認証に使用される場合、ID回復のオプションとして、モバイル・デバイスまたはメールアドレスに送信されたメッセージの検証を含めることができます。

オーセンティケーターとして、パスワード特異性の概念からパスワードレスへ移行するのは、旅のようなものです。オーセンティケーターの概念を採用している多くの組織は、強力なMFAがパスワードレス・ロードマップをサポートする基礎的な構成要素であることに気づいています。この旅には、適切な計画、実行、検証が必要ですが、特に今日のハイブリッド運用モデルにおいては、本人確認が新たなセキュリティの境界線となるため、得られるセキュリティ上のメリットとリスク低減は非常に重要です。

サイバー保険に加入する際のリスクを最小限にするには

米国の銀行は、2021年に1,489件のランサムウェア取引を特定し、計12億ドルの支払いを規制当局に報告しています。これは前年の報告数487件、計4億1600万ドルから急増しています[4]。

ランサムウェアの支払い額は2020～2021年に2倍以上に増加したため[1]、保険会社の損失が拡大し、サイバー・セキュリティ保険市場は一時期不安定となりましたが、最近ようやく安定してきています。2022年末にはサイバー保険料率の上昇が80％減速し、2023年の市場見通しは改善したものの[2]、ランサムウェアが依然として最大の脅威であることから、多くの保険会社はサイバー・リスクが引き続き上昇すると考えています[3]。その結果、企業の保険契約プロセスの際には、サイバー・リスクに関するセキュリティ対策機能および内部プロセスや手順についていっそう厳しく精査されることが予想されます。さらに、広範なイベント（Log4jなど）や、ウクライナ戦争や国家が支援する攻撃グループに関連するインシデントについては、厄介な除外項目が依然として残っています。実際、保険会社では、組織がこのリスクを管理するための適切なセキュリティ対策機能を実証できない場合、ランサムウェア関連の補償を削減あるいは除外する傾向が続いています。

過去12か月間でMandiantは、インシデントレスポンス業務においてサイバー保険会社の関与が増加していることを確認しています。CISO（最高情報セキュリティ責任者）は保険の適用範囲の決定において必ずしも関与していませんが、Mandiantでは、侵害を受けた時に予想外の事態にならないようにするため、CISOが組織のリスク・マネージャーや法務責任者と協力して、保険申し込みプロセスの正確性を確保し、保険契約内容を見直すことをお勧めしています。

サイバー保険の基礎知識

2000年代半ば、保険会社は、業務に直接影響を与えるサイバー攻撃のコストを企業に払い戻す補償を拡大しました[5]。以来、補償の拡大は、財務リスク・マネージャーやサイバー・セキュリティ・リーダーにとって、データ漏えいなどのセキュリティ・インシデントによるリスクを軽減し、コストを相殺するための有用なツールとなっています。一般的に保険は、企業に対するサイバー・リスク（第一当事者リスク）と、消費者や企業からの請求に対する賠償責任（第三者賠償責任）をカバーします。当初、サイバー保険の引受はデータ漏えいに関連するコストに重点を置いていたため、組織は、処理する記録の種類、顧客データ、規制対象データに関する情報を保険会社に提供し、HIPAAやPCI DSSなどの規制基準への準拠を証明する必要がありました。ランサムウェアと多重脅迫は事業中断の追加リスクをもたらし、業務を麻痺させ多額のコストを発生させる可能性があります。

1. Wall Street Journal, Reported Ransomware Incidents, Cost Soard in 2021, Treasury Says, November 4, 2022
2. Marsh, US Cyber Insurance Market Update Signs of improvement in third quarter of 2022, October 7, 2022
3. Woodruf Sawyer, 2023 Property & Casualty Looking Ahead Guide, January 10, 2023
4. Wall Street Journal, Reported Ransomware Incidents, Cost Soard in 2021, Treasury Says, November 4, 2022
5. The Federal Reserve Bank of Chicago, Chicago Fed Letter, No. 426, 2019 The Growth and Challenges of Cyber Insurance, 2019

表1：一般的なサイバー・セキュリティ・リスクの補償内容

第一当事者補償	第三者賠償責任
インシデント対応とフォレンジック料金	セキュリティおよびプライバシー賠償責任
通知、信用、個人情報の監視	マルチメディア/マスコミ連絡の賠償責任
データ回復	規制当局への対応と罰金
事業中断	PCI DSS賠償責任
サイバー恐喝とサイバー犯罪	電話消費者保護法への対応
社会的信用の失墜	

*出典：Honigman LLP Attorneys and Counselors, Cyber Insurance 101, May 19, 2021

その結果、保険会社は、事業中断やその他の関連する事業損失に対する組織の技術的セキュリティ対策機能や被害回避活動に注目し、より徹底的に精査するようになっています。すなわち、リスクと保険料金を決定する際の引受プロセスの基準が厳しくなっています。現在、保険引受の際には、追加の質問や面接、組織環境の外部的調査の提出が求められます。

Woods Rogersでサイバー・セキュリティおよびデータ・プライバシー業務の責任者を務めるBeth Burgin Waller（ベス・バーギン・ウォラー）氏（インシデント対応法律顧問であり、顧客のためのサイバー保険の内容確認と交渉に豊富な経験を有する）は、リスク管理チームや法務部門と協力して引受プロセスに備えることを推奨しています。

引受の際の調査票には、昨今の複雑なマルチ・クラウド、マルチ・ネットワークの企業インフラに必ずしも当てはまらない、イエス/ノーの質問がしばしば含まれています。例えば、企業全体で多要素認証（MFA）を行っているかという質問に答える際、保険会社は、バックアップからクラウド業務アプリケーション、VPNに至るまで、企業のあらゆる部分でMFAが存在することを証明するよう求めることがあります。組織の法務責任者やリスク管理チームの支援により、保険申請書に記載されている重大な記述に注意を払い、現在の本番環境の対策機能と改善計画を明らかにする補足的な回答を作成することができます。

インシデント対応補償のニュアンスを理解する

Burgin Waller（バーギン・ウォラー）氏は、見本（サンプル）保険契約を確認するよう強く推奨しており、「市場が安定するにつれて、サイバー保険の文言も他の保険商品と同様に標準化されつつあります」と語ります。見本の保険契約には、一定の限度額まで事業中断の補償があることが記載されていますが、注意深く調べないと、レガシー・ソフトウェアや、Log4jなどの広範な事象、あるいは最近の除外事項として、戦争行為（国家支援の攻撃者に起因するインシデントも含む）などについて保険契約に組み込まれている場合があります。Burgin Waller（バーギン・ウォラー）氏は、保険契約のサブリミット（特定の危険に対して通常の支払限度額より低い金額で設定される支払限度額）に特に注意を払うよう勧めています。ある例では、基本的なサイバー保険契約にフィッシングによるインシデントのサブリミットが含まれており、ランサムウェアに対する補足的な補償は組織が行うことを求められていました。Burgin Waller（バーギン・ウォラー）氏によると「初期段階でサンプル保険契約を注意深く読むことで、インシデントが実際に起こる前に、何が保険でカバーされ、何がカバーされないのかを明確にし、インシデント発生時の手間を大幅に減らすことができます」

インシデント対応プロバイダー費用やそれに関連するコストはカバーされるのでしょうか？Mandiantインシデント対応担当者の観察によれば、これには3つのシナリオがあります。

1) インシデント対応プロバイダーが、事前交渉済み料金で承認されたベンダーである。この場合は、契約の開始が効率化され、保険請求の提出が容易になります。

2) インシデント対応プロバイダーが承認済みベンダーではなく、保険会社は時間当たりの料金で費用を補償する。インシデント対応の料金が保険補償額を上回る場合は、保険加入者側が差額を補填する必要があります。

3) インシデント対応プロバイダーが承認済みベンダーではなく、そのプロバイダーを利用した場合、保険会社は補償を行わない。このシナリオでは、侵害イベント時に大きな混乱を引き起こす可能性があります。

インシデント対応プロセス全体をカバーするために、サンプル保険契約を確認することが重要です。保険によっては、調査のみを補償対象とし、ランサムウェアの支払い、顧問弁護士費用、復旧や長期的な修復作業に関連する費用は除外されています。さらに、攻撃者がどのように侵入したかを正確に判断し、再感染を引き起こしやすいバックドアが残されていないことを確認するための完全な調査については、保険会社がカバーしない場合があります。この場合は、将来のリスク低減を目的とした徹底調査を進めるかどうかについて、経営判断が求められることになります。

新しいアプローチ

サイバー保険市場は全体的に成熟しつつあり、プロバイダーは顧客と提携して全体的なサイバー・レジリエンスを強化するようになっています。保険業界には非常に高度なリスク・モデリング・プログラムがあり、これを適用して組織の安全性を高めるようになっています。

多くの保険会社は、保険加入者向けに、吟味済みのベンダーやソリューションのセットを提供しています。これにより保険加入者は、サイバー・セキュリティ市場を知り、有効性が実証された技術を採用することでリスクを低減できるようになります。

保険会社はさらに、組織のサイバー・リスクや関連する保険コストにプラスの影響を与えることができるセキュリティ対策機能も特定しています[6]。Mandiantでは、保険業界からの提言をもとに、以下の5つの実践方法を紹介しています。これらを適切に実施することで、典型的な攻撃の影響を軽減したり、防止したりすることができます。

1. **多要素認証：**MFA（二要素認証）とは、2つ以上の独立した認証情報（パスワード、セキュリティ・トークン、顔や指紋など）を組み合わせてユーザー・アクセスを提供する技術です。Mandiantが多くのインシデントレスポンス調査を通じて観察したところによると、組織は従来のMFA手法の採用を増していますが、一方で攻撃者は、個人情報を侵害する高度な戦術を継続的に展開していることがわかりました。外部アクセス可能なすべてのログイン・ポータルと機密性の高い内部アプリケーションに、番号照合、コンテキストに応じたテレメトリー通知、時間ベースのワンタイム・パスワード（TOTP）の入力など、強力なMFAツールと方法を導入することで、攻撃者の一般的な初期アクセス手法のリスクを低減することができます。
2. **本人確認と特権アクセスの管理：**今日のハイブリッドな運用モデルにおいて、本人確認はセキュリティの新たな境界線となっています。Mandiantは、多くのインシデント対応業務において、ディレクトリおよびアクセス管理システムの侵害を目の当たりにしています。これらのシステムは、攻撃者が権限昇格のためにしばしば使用します。組織は、ユーザーとシステムが適切なアクセス権を有していて、ディレクトリとアクセス管理システムが適切に設定されていることを確認し、不正な権限昇格を防止する必要があります。
3. **バックアップのセキュリティ確保、暗号化、テスト：**Mandiantでは、サイバー攻撃を受けた場合にシステムやデータの復旧を容易にするため、バックアップのセキュリティを保護し暗号化するためのテスト済みプランを備えるよう推奨しています。バックアップと外部ストレージのソリューションは、IP損失の可能性を減らし、貴重な記録を損失から確実に保護するのに役立ちます。企業は、サイバー攻撃によって業務が停止した場合に備えて、クラウドまたはハイブリッドのネットワークのコピーを維持する方法として、クラウド・サービス・ソリューションを利用することが増えています。

6. Marsh, Cyber Insurance Market Overview: Fourth Quarter 2021, December 7, 2021

4. **サイバー・インシデント対応の計画とテスト：**Mandiantは、サイバー・インシデント対応の計画とテストが重要な活動であると考えています。これには、既存の技術的セキュリティ対策機能、ネットワーク・アーキテクチャ、初動対応能力のレビューが含まれます。Mandiantでは、典型的な対応シナリオを想定した計画を策定し、インシデント発生時に迅速に封じ込めることができるよう、サイバー防御能力の検証を継続的に行うことを提案しています。

5. **法的およびインシデント対応パートナーの保持：**サイバー・インシデント対応計画で重要な部分の1つが、法的リスクから会社を保護し、インシデント対応に関する専門知識を得るため外部のサポートを受けられるように準備しておくことです。法務責任者（特にサイバー問題専門）は、攻撃時にフォレンジック対応者とシームレスに連携し、法的責任や事象から生じ得るリスクを評価できるようにする必要があります。外部のインシデント対応支援は、対応時間を大幅に短縮し、侵害の影響を軽減することができます。インシデントレスポンス・リテイナー（IRR）サービスでは、インシデントレスポンス・サービスの契約条件を、サイバー・セキュリティ・インシデントの発生前に話し合って決めておくことができます。

また保険会社は、セキュリティに関するコンサルティングや、申請手続きを支援するサービスも提供しています。多くの保険ブローカーや保険会社は、効果的な防御能力を開発するために必要な評価、サイバー衛生管理、プロセスなどのコンサルティングを拡張することで、サービスの差別化を図っています。

サイバー保険に関するお役立ち情報は、Mandiantの提携パートナー、ポッドキャスト、Webセミナー、Google Cyber Riskのオファーを参照してください。

セキュリティ・アナリストのケーススタディ：ソフトウェア・サプライチェーン侵害を見つけ出して阻止する

検知・対応機能を活用するメリット

昨年Mandiantは、サプライチェーン侵害が大幅に増加したことを報告しました。サプライチェーン内で始まった侵害は、2021年の侵害のうち17%となり、1%未満だった2020年から増加しています[7]。この増加は、Mandiantが追跡した侵害侵入の86%がSolarWinds侵害とSUNBURSTに関連していたという事実で部分的に説明がつきます[8]。しかしながら、この増加は、ベンダー244社と技術的な関係を維持している組織にも相関関係が見られます[9]。

ソフトウェア・サプライチェーン攻撃は目新しいものではありません。2017年、NotPetyaと呼ばれる攻撃が世界を襲いました。ランサムウェアに見せかけたこの不正コードは、NSAが流出させたEternalBlueの脆弱性を悪用してネットワークに侵入し、その後データを組織的に破壊しました。NotPetyaの背後にいる攻撃者は、ウクライナ政府のサプライヤーであった金融サービス・ソフトウェア会社を侵害しました。

同年、ユーティリティCCleaner[10]が侵害を受け、ハッカーがソフトウェアの正規版を不正なものに置き換えたため、200万以上のホストが危険にさらされました。

2020年、SolarWindsのコンポーネントを活用した前述の広範な攻撃は、APT29（以前の名称はUNC2452）によって実行されました。このグループの標的は、ロシアの戦略的利益に合致すると評価されています[11]。APT29の影響を受けた被害者は、政府機関やフォーチュン500社など多岐にわたっています。今回も攻撃者はソフトウェア・サプライチェーンをターゲットに、ソフトウェア・コンポーネントOrionにバックドア・コードを注入して、被害者の内部環境にアクセスできるようにし、正規のプロセスでアップデート・コードが配布された後にSUNBURSTマルウェアを展開することができました。

攻撃者は、デジタル企業の基盤となる構築要素を侵害する方法を発見しています。ソフトウェア開発者が使用する一般的なパッケージを標的とし、侵害に成功することで、不正コードを被害者に直接配布し、これを大規模に増幅させることが容易になっています。このアプローチでは、防衛側の私たちが、いかに防御態勢の準備ができているかが問われています。世界中の組織が、攻撃経路の可視化と、検知・対応機能の信頼性を維持するための取り組みを続けています。多くの組織は、ソフトウェア・サプライチェーンにおけるサイバー攻撃を迅速に察知し阻止する能力について、確信を持てていません。その理由の1つは、適切な訓練を受けたセキュリティ専門家が不足しており、訓練や知識の見直しに十分な頻度での活動や対応ができないためです。

7. Mandiant『M Trends』2022年
8. Mandiant『M Trends』2022年
9. Mandiant『防御側の優位性 - サイバー・スナップショット』第2号、2022年
10. Mandiant Threat Intelligence, "CCleaner Supply-Chain Compromise Possibly Linked to Chinese Cyber Espionage Operators", September 2017
11. Mandiant, "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor", December 2020

ソフトウェア・サプライチェーンの侵害は、サードパーティ・プロバイダーへの信頼を悪用して、被害者の環境に間接的にアクセスすることを目的として設計されており、検知が困難な場合があります。最終的には、セキュリティ・アナリストの訓練された目と調査プロセスが、高度な攻撃を特定し阻止する決め手となります。

サプライチェーン攻撃では、信頼関係が事前に確立されているため、不正なインプラントを直接検知することは極めて困難です。有効で効果的な検知能力と対応能力が何より重要になります。攻撃ライフサイクルの最後の段階になって疑わしいイベントが検知されたときに、アナリストが調査を通じて攻撃者の行動を巻き戻すことで、間接的にインプラントを発見することができます。

—Steve Ledzian（スティーブ・レジアン）、CTO-APAC担当バイスプレジデント、Mandiant

アナリストによるソフトウェア・サプライチェーン侵害の検知と調査

2021年10月中旬から、Mandiantのマネージド検知・対応サービスのセキュリティ・アナリストが、オープンソース・リポジトリの侵害と思われる複数の事象を確認しています。以下の事例では、その検知および調査プロセスと、解明に取り組んだ疑問点について説明します。この事例には、JavaScriptプラットフォームNode.jsのパッケージ・マネージャーであるNode Package Manager（NPM）上でホストされているパッケージが関与していました。

Mandiantセキュリティ・アナリストの小規模チームが最初に複数のアラートを観察しました。これは、ネイティブのWindowsユーティリティ**CERTUTIL.EXE**が、共通のURL **(hxxps://citationsherbe[.]at/sdd.dll)** からペイロードをダウンロードするために使用されているというものでした。セキュリティ・オペレーション・センター（SOC）のアナリストが同様のアラートを検知することが増えたため、このチームは疑問解決の調査のため連携して取り組みを始めました。

いったい何が起きているのか？ どのようにしてシステムにダウンロードさせているのか？

最初に答えるべき疑問は、「どのようなマルウェアが存在し、その能力はどのようなものか」、そして「どうやってシステムに到達したのか」です。アナリストたちは、疑わしいバイナリの機能と能力を調べるために、最初のホストからペイロードを取得しました。トリアージ解析の結果、このバイナリはDANABOTマルウェアの亜種であり、攻撃者が管理するコマンド＆コントロール（C2）サーバーとの通信を介して、認証情報を盗むことを目的としていることが判明しました。マルウェアのC2アドレスを使って、アナリストたちは攻撃者インフラと通信している他のシステムを特定することで、環境の範囲をさらに広げていきました。このプロセスにより、アナリストたちは、同じまたは類似のマルウェアが、対応するアラートがないまま他のシステムに展開された可能性があるかどうかを判断できます。このペイロードがマルウェアであることが確認されると、アナリスト・チームは、リモートで、またはインシデント対応チームに対応を開始させることで、侵害されたホストを封じ込める作業を進めました。

DANABOTはDelphiで書かれたバックドアで、TCP上のカスタムバイナリプロトコルを使用して通信します。このバックドアはプラグイン・フレームワークを実装しており、ダウンロードしたプラグインを経由して機能を追加することができます。DANABOTの機能には、VNCやRDPプラグインを使ったシステムの完全制御、動画やスクリーンショットのキャプチャ、キーロギング、任意のシェルコマンド実行、ファイル転送などがあります。DANABOTのプロキシ・プラグインにより、標的のWebサイトに関連するネットワーク・トラフィックをリダイレクトしたり操作したりすることができます。この機能は、認証情報や支払いデータを取得するためによく使用されます。DANABOTは、WebブラウザやFTPクライアントに関連した保存済み認証情報を抽出することもできます。

「ua-parser-js」は軽量かつ小さなフットプリントのパッケージで、Webアプリケーションまたはサーバー側アプリケーション内に配置され、User Agent文字列（Browser、Engine、OS、CPU、Deviceなど）の解析に必要な関連データを抽出してフィルタリングします。

侵入経路は？

マルウェアがどのように展開されたかを理解するために、アナリストは通常、エンドポイント検知・対応（EDR）技術によって収集されたデータを利用します。EDRのテレメトリーを確認することで、アナリストたちは、NPMパッケージをアップデートするためにユーザーが実行した正当なコマンドのアクティビティを突き止めました。

徹底的な調査の結果、**UA-PARSER-JS PACKAGE**ディレクトリに同様のファイルが書き込まれていることが判明し、アナリストたちはこのホストが侵害されてマルウェアを配布していると考えました。JS Packageディレクトリを不正に変更したことで、パッケージのインストール・プロセスにプリインストール・ステップが追加され、マルウェアがダウンロードされたのです。侵害されたスクリプトをアナリストたちが検証したところ、コインマイナー（暗号通貨マイナーとも呼ばれる）をホストにダウンロードし、展開していることも分かりました。このパッケージ・リポジトリのGitHub Issuesを確認したところ、誰かが「このパッケージはごく最近侵害されたのか」と質問しているのを発見しました。2021年10月22日12:15 UTCごろに提起されたGitHub Issueによれば、週700万を超えるダウンロードがある人気のNode.jsライブラリであるNPMパッケージ**「ua-parser-js」**が、マルウェアを配信するよう侵害されていました。攻撃者は、作成者のNPMアカウントを乗っ取ることで、3つの不正バージョンのパッケージを公開することができました。リポジトリのGitログによると、10月22日の16:14 UTCから16:25 UTCの間に、パッケージ作成者がさらなる侵害を阻止するために、不正パッケージのクリーン版をコミットしています。

この攻撃者は他にどのような活動を行ったか？

このホストを封じ込めた後も、アナリストたちは攻撃の根本的な原因を突き止めるために調査を続けました。パッケージ・リポジトリのGitログを確認したところ、不正な変更がプッシュされた時刻と、その数時間後に修正版が適用された時刻が記録されていました。さらに攻撃者のTTPを分析することで、同じ攻撃者によって侵害された追加のNPMパッケージが判明し、この攻撃者が行った活動の範囲を拡大して把握することができました。チームは、この活動をUNC3379に関連付けることができ、マルウェアの分析、攻撃者の行動の記録、今後の活動を阻止するための検知技術の開発を、妥当な信頼性で行うことができるようになりました。

このソフトウェア・サプライチェーン侵害の侵害に関する詳細は、調査ブログ：No Unaccompanied Miners: Supply Chain Compromises Through Node.js Packagesを参照してください。

アナリストの直感、批判的思考、経験を信頼する

調査では、その規模に関係なく、時間が勝負です。Mandiantでは、調査や対応の際に、アナリストの知識、これまでのトレーニング、批判的思考を頼りにしています。Mandiantのチームは探偵のように、手がかり、証拠、科学捜査の結果を活用して、それぞれのインシデントの背後にあるストーリーを解明していきます。調査プロセスの目的は、攻撃に関する重要な疑問に答え、以下の点を解明することです。

- 侵入の範囲
- 現在も継続しているかどうか
- 侵害された最も古い日付と侵害の原因
- 侵害にさらされたデータの種類と範囲
- 攻撃者の正体と動機

侵入に関するこのような事実を理解することが、封じ込め、根絶、復旧の指針となります。Mandiantでは、最前線での経験、シミュレーション、トレーニングを通じて、アナリストが調査を指揮し、封じ込めや根絶のタイミングや実行に関する重要な意思決定を行えるようにすることを推奨しています。Mandiantのバイスプレジデント、エリック・スケールズ（Eric Scales）はこう言っています。「インシデントの調査や対応を自社で行っている組織では、すぐ修復に飛びついてしまうことがよくあります。攻撃について理解すればするほど、根絶や復旧の成功率は高まります」

今回紹介したケースでは、Mandiant MDRのアナリスト主導の調査により、活動に関連する主要なアトミック・インジケーターを作成し、展開されたマルウェアのトリアージを実施して適切な修復措置を決定し、脅威グループに関する深い知識と研究を利用して、お客様の環境を把握し、お客様のEDR製品では検知できなかった今回のキャンペーンに関する他の悪質な活動も検知しました。

CISAのCross-Sector Cybersecurity Performance Goals（全業種サイバー・セキュリティ・パフォーマンス目標）でサイバー防御を活性化する

国家が支援する攻撃者は、依然として重要インフラ技術を狙っています。昨年Mandiantでは、攻撃者がオペレーショナル・テクノロジー（OT）・ネットワークでアクセスを確立した後、特定の産業制御システム（ICS）または監視制御およびデータ収集（SCADA）デバイスをスキャン、侵害、制御できるようにする、カスタムメイドのツールに関する調査結果を報告しました[12]。産業および重要インフラのネットワーク接続が進むにつれ、脅威の高度化が進み、重要インフラに対するサイバー・セキュリティ・ガイダンスの更新の必要性が高まっています。米国国土安全保障省サイバー・セキュリティ・インフラストラクチャー庁（CISA）、米国国立標準技術研究所（NIST）、および省庁間コミュニティは、すべての重要インフラ部門に一貫したサイバー・セキュリティ目標を策定しました。

2022年10月にCISAは、最も重要なサイバー・セキュリティの実践を特定し、優先順位をつけるのに役立つガイドとして、Cross-Sector Cybersecurity Performance Goals（全業種サイバー・セキュリティ・パフォーマンス目標）[13]を発表しました。CISA CPGは、組織が日々直面するサイバー・セキュリティの課題に対処するためのベースラインとなることを目的としています。病院、エネルギー供給会社、交通システム、主要製造業など、米国の重要なインフラの防御態勢を改善するために、サイバー・リスクを軽減するという共通の目標を達成することを目的としたものです。

Mandiantでは、CISA CPGガイドラインを受け入れ、リスクを低減するための出発点としています。CPGは、National Security Memorandum（NSM-5）「重要インフラ制御システムのサイバー・セキュリティを向上させる」に対する目標の最初の試行となります。これは、包括的なサイバー・セキュリティ・プログラムではなく、より強力なサイバー・セキュリティの実践に向けた道を歩み始めるための重要なステップです。

12. Mandiant、『INCONTROLLER：複数の産業用制御システムを標的とする新たな国家支援型サイバー攻撃ツール』、2022年4月13日
13. Cybersecurity and Infrastructure Security Agency, CPG Cross-Sector Cybersecurity Performance Goals 2022

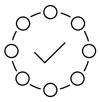
CPGは、サイバー・リスクを低減するための目標ではなく、最低限の基礎となるものです。主な特徴的ハイライトは以下の通りです。

サイバー・セキュリティ実践のサブセットのマッピング

ITとOTに特化した関連ガイドライン

優先順位付けを行ったリスク低減実践

CISAとその産官パートナーが観測した脅威から情報を得る



すべてのCI（重要インフラ）部門に適用される

CPGは、これらの組織が重要なインフラをよりよく守るための方法として、OTとICSに関する具体的な行動と項目を呼びかけています。

組織の規模を問わず、重要なインフラを保護するためには、関係するサイバー脅威を把握し、厳しいセキュリティ・テストを実施し、脅威の検知と対応を組織全体にわたって徹底する必要があります。CPGは、予算、スタッフ、専門知識を考慮しながら、最もインパクトのあるセキュリティの成果に向けてどのように投資を集中させるかについての検討を支援します。CPG実施のための実践への投資は、「アメリカ国民の安全、健康、生活に対する重大なリスクに有意義に対処するのに役立ちます[14]」

14. Cybersecurity and Infrastructure Security Agency, CPG Cross-Sector Cybersecurity Performance Goals 2022

関連するサイバー脅威を理解する

CPGは、自組織に関連する脅威の認識を維持し、攻撃者の戦術、技術、手順（TTP）を活用して進行中の攻撃を検知するガイドとなります。MandiantのOTセキュリティに対するアプローチにおいて、関連するサイバー脅威を理解することが最も肝要です。ITとOTの両方のネットワークの脅威検知能力を強化し、完全な状況把握を実現するよう、お客様をガイドするものです[15]。防衛側やインシデント対応者は、攻撃のライフサイクルにわたる侵入手法（TTP）にもっと注意を向けるべきだとMandiantでは考えています。TTPの多くは、ITとOTのネットワーク境界を越えるシステム、あるいはOTネットワーク内のネットワーク接続されたワークステーションやサーバーで、ITで使用されているものと類似（または同一）のオペレーティング・システムやプロトコルを使用しているもので、我々が「中間システム」と呼んでいるものの中に存在します。高度なOT攻撃の大半は、この中間システムを最終ターゲットへの踏み台として活用するため、侵入方法に焦点を絞ることが効果的です。

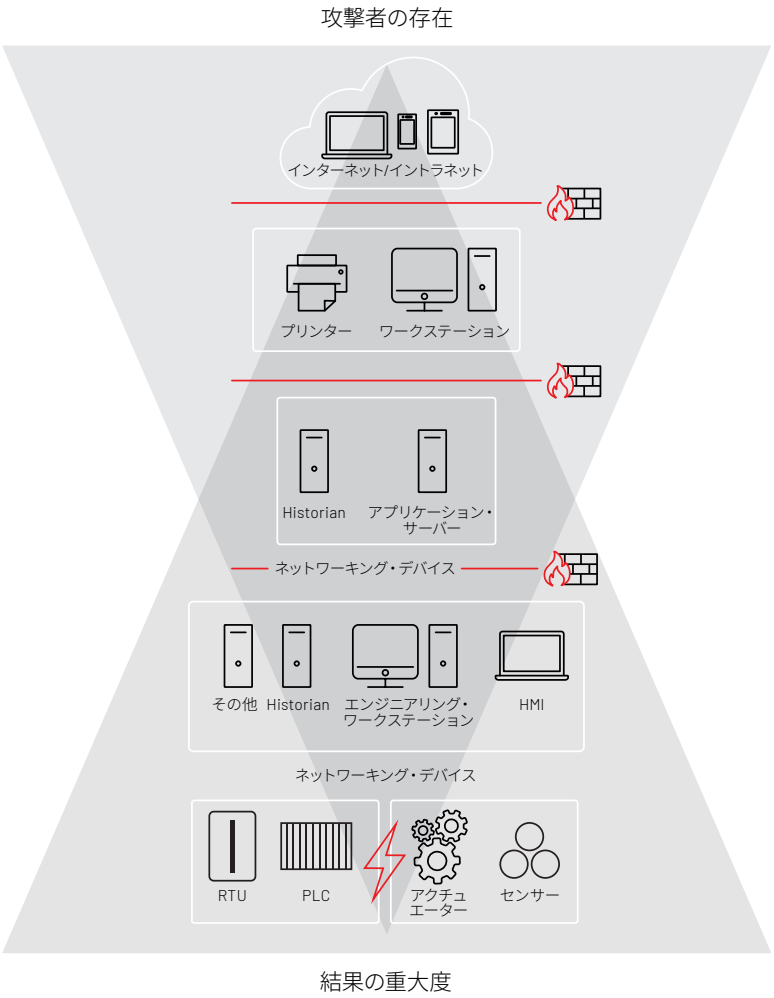


図1： OT脅威の検知における機会ファネル

15.Mandiant, The Mandiant Approach to Operational Technology Security, December 2019

標的型OT攻撃者を検知する最大の機会は、図1の2つの三角形の間の重なった部分にあります[16]。攻撃者の存在と侵入による業務上の影響のバランスがとれているため、セキュリティ組織が脅威の活動を特定することが容易になり、より有意義なものとなるのです。防御側は、攻撃者の侵入方法を理解し、その知識を活用して高度な脅威ハンティングと検知を行う必要があります。OTのDMZと分散制御システム（DCS）の近くで脅威ハンティングを行うことは、検知可能な侵入機能がまだ存在し、侵入の潜在的な結果の深刻度が高いけれどもまだ致命的ではないため、最も効率的である可能性があります。

16. Mandiant, The Mandiant Approach to Operational Technology Security, December 2019

2022年

Mandiantは2022年、ランサムウェアによる恐喝攻撃で機密性の高いOTドキュメントおよびネットワーク・ドキュメントが漏出したことを報告しました[17]。ランサムウェア関連やあらゆるタイプのデータ漏えいによって機密性の高いOTデータが漏出することで、高度な攻撃者は、ターゲットに関する情報、特に被害者のインフラ、資産、セキュリティの弱点、およびプロセスに関する情報を得ることができます。この種の偵察データは、攻撃者がより重大な影響がありかつ正確な攻撃を行うために使用されます。

表2：ランサムウェアによる恐喝攻撃で漏えいした文書

被害者（実名は伏せる）	漏えい内容
産業用・旅客用鉄道車両の製造メーカー	OEMのパスワード管理認証情報、欧州の路面電車車両の制御アーキテクチャと通信チャネルの要件、Siemens TIA Portal PLCプロジェクト・ファイルのバックアップ、など。
石油・天然ガス関連の2団体	図、HMI、スプレッドシートなど、ネットワークおよびプロセスの詳細な文書。
制御システム・インテグレーター	顧客プロジェクトの技術文書（一部のファイルはパスワードで保護されていたが、バイパスはされなかった）。
水力発電事業者	ほとんどのデータは財務・会計関連だったが、IT部門、プラント・メンテナンス部門、オペレーション部門の従業員の名前、メール、ユーザー権限、一部のパスワードのリストが確認された。
衛星による車両追跡サービス事業者	全地球測位システム（GPS）経由で自動車群を追跡するために使用されている独自技術プラットフォームの製品図、視覚化、およびソースコード。
再生可能エネルギー事業者	再生可能エネルギー・インフラの保守・供給に関する条件を記載した、被害者と顧客との間の法的契約。契約書には、サービス・プロバイダーがパブリックインターネットIPアドレスを通じてサードパーティのSCADAシステムにフルアクセスできることが記載されていた。

- ネットワークのすべてのセグメントのデータに触れる従業員や請負会社に対して、堅牢なデータ取り扱いポリシーを実施し、内部文書の保護を徹底する。
- 機密性の高い業務データを安全性の低いネットワークに保存することは避ける。
- 業務データを保護するための包括的なセキュリティ・プログラムを実施している請負会社を選定するよう特に注意する。
- ランサムウェア侵入の被害者は、漏えいしたデータの価値を評価し、さらなる侵入のリスクを低減するのにどのような代償措置が役立つかを判断する必要がある。
- 漏えいした認証情報およびAPIキーを変更する。リスクにさらされた重要なシステムやOTジャンプ・サーバーのIPアドレスの変更を検討する。
- レッドチーム演習を定期的に行い、外部にさらされている安全でない内部情報を特定する。

17. Mandiant、『ランサムウェア攻撃の7件に1件で重要なOT情報が流出』、2022年1月

厳しいセキュリティ・テスト

OTネットワークのセキュリティ態勢を確実に向上させる鍵の1つは、重要な資産を狙う最も一般的な攻撃やマルウェア・ファミリーに対して、OTネットワークの各レイヤーでセキュリティ制御を安全にテストすることです。CISA CPGでは、組織のサイバー防御の有効性と適用範囲について、定期的に第三者による検証を行うことを推奨しています。

Mandiantでは、組織の評価ニーズに合わせてカスタマイズされたプログラムをアドバイスしています。OTの包括的なテストプログラムは、攻撃者の視点から実施し、シミュレーションとエミュレーションを活用してリアルタイムの運用への影響を軽減し、レッドチーム、パープルチーム、ペネトレーション・テスト、ネットワークおよびコンポーネントのセキュリティ・テストの組み合わせを適切に取り入れたときに最も効果的になります。本番のOT環境における運用のアップタイム要件により、防御態勢テストができない場合、Mandiantでは、ネットワークのセグメンテーション、アクセス管理、ネットワーク監視システム、過渡的デバイス・ポリシー、インシデント対応能力の有効性を評価する技術評価を推奨しています。継続的にテストを行うことは、ある時点でのセキュリティ対策の有効性を評価するだけでなく、攻撃者に悪用される前に、統合されたネットワーク（ITからOTまで）全体の複雑なセキュリティ問題を特定するのに役立ちます。継続的な検証は、組織のチームがサイバー・インシデントを監視、検知、対応するための準備にもなります。これらのプログラムにより、重要な発見を軽減するための戦術的な推奨、長期的な改善のための戦略的な推奨、OTインシデントを監視し対応するスタッフの能力におけるギャップの特定という利点が期待できます。

Open Platform Communications サーバーは、産業環境内の機械、デバイス、システム間で、メーカーに依存しない類似のデータ交換を可能にします。

対応と復旧

CISA CPGのセクション7では、関連する脅威シナリオに対して組織がサイバー・セキュリティ・インシデント対応計画を維持、実践、更新する必要性が概説されています。Mandiantは、TRITONやINCONTROLLERといった大規模なOTインシデントの最前線で対応した経験から、ITインシデント対応とOTインシデント対応の違い、OT対応に必要なツールや手順について深く理解しています。

IT環境とOT環境では、修復と封じ込め（脅威を環境から排除し、システムを通常の運用状態に戻すこと）の目標は同じですが、ツールは大きく異なります。IT対応の場合は、調査、封じ込め、復旧/修復を支援するために、エンドポイント検知・対応技術を日常的に使用しています。これらのツールは、通常、OTネットワークのサーバーやコンポーネントにインストールされることはありません。

ITにおける封じ込めは比較的簡単で、複雑なOT環境での封じ込めに比べ、はるかに影響が少ない場合がほとんどです。例えば、ITネットワーク上で特定の機能を停止・起動したり、システム全体を削除したりすることはよくあることです。このような作業は、OTコンポーネントで行うと、影響がずっと大きくなることがあります。重大なダウンタイムや、生命の安全を脅かす可能性のあるオペレーションに影響を与えることなく、プロセスを開始または停止したり、コンポーネントをオフラインにしたりする場合は、あらかじめ、基礎となるプロセスを包括的に理解する必要があります。例えば、OPC（Open Platform Communication）サーバーは、無造作にオフラインにすると、製造ライン全体に数週間の影響を及ぼす可能性があります。詳細な計画（実際のインシデント対応とは別に）は、システム所有者が潜在的なダウンタイム、生産損失、生命安全のリスクに基づいて、リスクベースの意思決定を行うのに役立ちます。潜在的な攻撃者の目標と目的を理解することは、システム所有者がより安全でリスクの少ない意思決定をするための指針になります。

最後に、OTネットワークは、組織が直接アクセスできない、多くのベンダーが運営するサブネットワークで構成されています。Mandiantでは、サードパーティのシステムを取り入れた対応計画やプレイブックを作成し、それらのベンダーと連携してテストすることを推奨しています。サイバー・セキュリティ・インシデントを迅速、効率的、大規模に解決するための計画を用意し、それを実践することの重要性は、いくら強調しても言い尽くせないほどです。

Mandiantは、NISTサイバー・セキュリティ・フレームワークの5つの機能[18]（CISA CPGがこれを補完している）にOTセキュリティ・サービスをマッピングし、組織のサイバー・セキュリティ・リスク管理のライフサイクルにサービスを適合させています。

18. NIST, Cybersecurity Framework, The Five Functions, May 2021

		特定	保護	検知	対応	復旧
インテリジェンス	インテリジェンス・サブスクリプション	■	■	■		
	専任のインテリジェンス・アナリスト	■	■	■		
	脆弱性診断サービス	■	■			
	カスタム分析とブラックボックス評価	■				
コンサルティング	ヘルスチェック	■	■	■		
	セキュリティ・プログラム診断サービス	■	■			
	攻撃およびペネトレーション・テスト	■	■	■		
	インシデント対応計画	■			■	■
	インシデント対応				■	■
	セキュリティのトレーニング	■	■			
	専任のコンサルタント	■	■	■	■	■
Managed Defense for OT	ジャンプスタート	■	■			
	継続的なモニタリング		■	■	■	
サードパーティ・テクノロジー	OTネットワーク・プロトコル・モニタリング	■		■		

図2：MandiantのOT向けサービス

Mandiantは、ICSおよびOT環境での数十年にわたる実務を通じて得た産業用制御システムの深い機能的知識により、最前線のサイバー・セキュリティに関する知見を提供します。MandiantのOT専門家は、高度なセキュリティ・テストを実施し、産業組織がエンドツーエンドのOTネットワーク全体で回避・検知能力を向上させるのを支援します。より安全なOT環境とサイバー対策準備の向上のために、CISA CPGをマッピングするお手伝いをいたします。

最後に

今号の『防御側の優位性 - サイバー・スナップショット』では、従来のパスワードや多要素認証（MFA）からパスワードレス認証の導入へと進む組織に対して、強力なMFA方式をベースに、すべてのデバイスやアプリケーションへのバックエンド認証を仲介するサードパーティ製シングル・サインオンをぜひ検討するよう説明しています。Mandiantは、不安定なサイバー保険市場において、保険申込書の作成に法務責任者やリスク管理者を加えること、サンプル保険契約を慎重に検討すること、保険会社を全体的なリスク管理のパートナーとして注目することを提案します。

さらに、『防御側の優位性』で説明されているサイバー防衛の6つの重要な機能が、米国サイバー・セキュリティ・インフラストラクチャー庁（CISA）が最近発表した「Cross-Sector Cybersecurity Performance Goals（全業種サイバー・セキュリティ・パフォーマンス目標、CPG）」で提供したガイドラインと一致していることを実証しています。これらは、重要インフラの所有者や運営業者が、リスクを大幅に低減するために実施できるサイバー・セキュリティの実践を示すものです。また、最適化されたSOCが展開する戦術の例として、アナリストが関連するアラートを統合的な調査として調べ、アナリストの訓練、経験、批判的思考に頼りにサプライチェーン攻撃を調査するケーススタディを取り上げています。

知識はサイバー攻撃者に対する戦いにおいて、最大の利点の1つです。『防御側の優位性 - サイバー・スナップショット』は、セキュリティ・チームに伝え、リーダーによるスマートな意思決定を可能にする知見とインテリジェンス、ただそれだけを提供することを目指しています。サイバー・セキュリティ業界は、情報を共有し、対応者がこの戦いを続けられるように協働する必要があります。『防御側の優位性 - サイバー・スナップショット』は、こうした努力をサポートするMandiantの取り組みのうちの1つです。

詳しくはwww.mandiant.jpをご覧ください。

マンディアント

〒100-0006 東京都千代田区有楽町1丁目1番2号
東京ミッドタウン日比谷 日比谷三井タワー12F
03-4577-4401

japan@mandiant.com

Mandiantについて

Mandiantは、ダイナミックなサイバー防御、脅威インテリジェンス、インシデントレスポンスサービスのリーダーとして知られています。長年にわたり攻撃の最前線で得た豊富な経験を活かし、サイバー脅威に対する防御と対応においてお客様組織を支援します。Mandiantは現在、Google Cloudの一部です。

MANDIANT
NOW PART OF Google Cloud