デジタルフットプリントの懸念、活用と対策

2021 年 7 月

名和 利男

1. デジタルフットプリントとは

デジタルフットプリントとは、インターネットやデジタル機器上で行われた、追跡可能なデジタルアクティビティ、アクション、投稿、通信の独自のセットのことで、組織のオンライン活動の結果としてインターネット上に存在する組織の情報のことである。組織のデジタルフットプリントは、恐るべき速さで拡大・変化し、従業員、サプライヤー、その他のサードパーティが、知らないうちに組織の機密情報を公開してしまっている。このような意図せず公開された機微性のあるデータは、組織を無防備にし、攻撃者が組織の情報とリソースを悪用するために利用されている。

このデジタルフットプリントには、次のような状況や課題がある。

- プライバシーの問題: デジタルフットプリントはデジタル ID やパスポートではないが、収集されたコンテンツとメタデータは、インターネットのプライバシー、信頼、セキュリティ、デジタルレピュテーション、および推奨に影響を与える。
- 採用活動への影響: テクノロジーが普及するにつれ、採用プロセスでのコスト削減とアクセスのしやすさを理由として、ソーシャルメディアでのやり取りを通じて応募者をデジタルフットプリントで評価する雇用者も増えている。 強力なオンラインプレゼンスは、生計を確保または維持するために重要な場合がある。
- 子どもへの影響: アルファ世代(ミレニアル世代の子ども世代、主に 2010 年以降生まれ)は、ネットとデジタル機器のテクノロジーなしには存在しない最初の世代である。そのため、子どものデジタルフットプリントはこれまで以上に重要になり、その結果は不明確になる可能性がある。子どものデジタルフットプリントは、意図されたオーディエンス(利用者、閲覧者)を超えてインターネットを横断する可能性がある。

2. デジタルフットプリントの監視によるリスク軽減

攻撃者が意図的に攻撃対象組織のデジタルフットプリントを収集利用して、より巧妙に組織へのダメージを仕組むことができる一方、防御する側も自組織と攻撃者のデジタルフットプリントを継続的に監視・管理することで、「外部デジタルリスク」を低減することができる。「外部デジタルリスク」のマネジメントは、サーフェスウェブ、ディープウェブ、ダークウェブにおけるリスクを継続的に監視するだけでなく、「外部デジタルリスク」に迅速に対応するためにも役立つものであ

© TOSHIO NAWA

る。

デジタルフットプリントの監視によって軽減できる主なリスクは、次のとおり。

1　サイバー脅威

2　経営陣への脅威

3　データ流出

4　ドメイン・フィッシング

攻撃者は、公開されたデジタル資産や効果のないセキュリティソリューションを悪用する手法を持っている。デジタル攻撃は、組織の機密情報を暴露し、時には攻撃者がこの情報をダークウェブ上のフォーラムで取引することもある。

サイバー脅威

- **マルウェア：** 標的のコンピューターにダウンロードされ、データを盗んだり、ファイルを暗号化して身代金を要求したりする悪質なソフトウェア
- **フィッシング：**メール受信者を騙してパスワード等の機密情報を入力させる偽サイトに誘導したり、その他の有害な行動を取らせるために作成されたメール
- **中間者攻撃：** 標的となるコンピューターを騙して攻撃者が仕掛けた危険なネットワークに参加させ、通信内容の盗聴や改ざんを行う攻撃

経営陣への脅威

ドクシング（Doxing）： 組織や特定の組織に所属する役員の個人情報や、個人を特定できる情報を調査して公開する行為

- **レピュテーションリスク：** SNS やソーシャルメディア上の意図的な炎上行為や、ジャーナリストへのリークにより組織や役員の評価を下げる行為
- **資格情報フィッシング：**経営陣が扱う可能性が高い、機微性のあるコンテンツへのアクセス権限の多いアカウントを狙うフィッシング行為

データ流出

攻撃者は、標的とする組織の顧客の認証情報や、組織の機密データにアクセスするために、組織のデジタルプレゼンス[1] に注目している。

---

[1] デジタルプレゼンスとは、Web サイト、ソーシャルメディアプラットフォーム、ビジネスディレクトリリスト、カスタマーレビュー、その他のオンラインソースなどを通じて、自組織のビジネスのアピールをすること。

また、攻撃者は、組織に知られていない未使用の公開サーバーでアプリケーションをホストすることもある。その際、標的型攻撃の踏み台やインフラ（フィッシング目的の偽サイトなど）として悪用される可能性がある。

ドメイン・フィッシング

資格情報のフィッシングでは、ブランド・ドメインを偽装する。例えば 1 つのアルファベットをよく似たギリシャ語のアルファベットに置き換えて偽サイトを作り、あたかも正規のブランド・ドメインのように見せかけてブランドの顧客から資格情報を得ようとする。

3. 攻撃者が積極的に利用するデジタルシャドウ

デジタルシャドウとは、デジタルフットプリントの一部で、個人情報、技術情報、組織情報などの機密性の高い情報のことを指し、組織を危険にさらすものである。攻撃者は、特定組織へのサイバー侵害のために、デジタルシャドウを積極的に利用している。

特に、多くのネットユーザーは、コンピューター、携帯電話、その他のデジタル機器を通じて、毎日、何百ものデジタルフットプリント（データ痕跡）を残している。そして、これらのデータが広く収集及び分析された上で形成されるプロフィールが、特定個人のデジタルシャドウとなる。SNS 投稿、ブログ公開、ファイル共有などで、意図的にネットに露出している情報だけではない。どのサイトを訪れたか、何を検索したか、どこからログインしたかなどの情報も含まれる。

組織のデジタルシャドウは、次のようなさまざまな形態をとっている。

- 内部の人間によってダークウェブのマーケットプレイスで販売される組織の機密情報
- 従業員によってコード共有サイトで公開された秘密の暗号キー
- フィッシングキャンペーンのでの利用価値が高い、幹部社員の個人情報
- 会社の本社の間取り図・設計図
- 一般公開されているシステム情報

これらの情報はすべて、攻撃者が組織にリスクをもたらす機会を与えるものである。セキュリティ実務者以外の方がデジタルシャドウについて理解する一助となるよう、Tactical Tech による動画を紹介する。

What is a Digital Shadow (https://vimeo.com/106165094)

4. デジタルフットプリントへの対策

デジタルフットプリントのアセスメント

オープンソースから入手可能なデジタルフットプリントを使用した攻撃が、企業のビジネスに影響を与え始めている。これをアセスメントすることで、ビジネスプロセスにおける「デジタルフットプリントの許容度」を見積もることができる。

このアセスメントは、オープンソースインテリジェンス（OSINT）技法により行うことができ、主な実施対象は次のとおりである。

- ソーシャルメディア上の情報
    - ソーシャルメディア（Google、Facebook、Twitter、Vkontakte[2]）に公開されている職務内容等、組織内部の「公開を前提としていない」情報など
- 開示されている機密性情報
    - インターネット（Google 検索結果、ブログ、フォーラムなど）上で入手可能な状態になっている、「機密技術データまたはその恐れのあるデータ」など
- 漏洩しているデータ
    - インターネット上或いはダークネット等で入手可能な状態になっている「会社のパー

[2] Vkontakte(フ コンタクテ)はロシア最大級の SNS で、月間アクティブモバイルユーザーは 7 千万人程度。

トナーに関するデータまたは社内使用のみのデータ」など

- メールアドレス及び連絡先のレビュー
  - ソーシャルエンジニアリング攻撃（フィッシング）で使用される可能性のある「オープンソースからの企業の電子メールアドレスおよびその他の連絡先情報」の識別など
- マルウェアおよび不審な挙動
  - ダークネット上で流通している「企業のサブネットワーク内のボットネット挙動」や「フィッシングや XSS などの脆弱性」の情報など
- ホスト（サーバー）上のデータ
  - ホスト（サーバー、デスクトップ、データベース）と使用中の「アプリ名およびバージョンに関する情報」の収集により、それらの脆弱性と公開エクスプロイトの存在や利用可能など
- ネットワーク上のデータ
  - サイバー空間で利用可能な「ネットワークアドレス、ネットワークデバイス、および関連する脆弱性に関する詳細情報」など
- ドメイン及び DNS 名に関する情報
  - 「ドメインと DNS 名」の受動的な識別とリストなど
- 攻撃に利用可能なメタデータ
  - 内部攻撃の開発に使用できる「Web ページコンテンツと企業リソースファイル」の収集と評価など
- 技術的な設定ミス
  - 攻撃者が不正アクセスを取得するために使用する可能性のある、Web サイトやその他の公的にアクセス可能なサーバー上の「既知の構成の脆弱性の特定」など

デジタルフットプリントの抑制策

攻撃者はサイバー侵害のためにデジタルフットプリントを利用するが、これを抑制するために企業や個人が行うことができる対策は、次のとおり。オンラインサービスやアプリを利用する限り、デジタルフットプリントを残さないようにすることは不可能であり、防御側がデジタルフットプリントのリスクを理解しコントロールすることが必要である。

- 個人は、すべてのオンラインサービスやアプリを利用する前に、それぞれのプライバシーポリシーを必ず通読し、「収集される情報」と「共有される範囲」を把握し、発生しうるリスクを理解すること。

- 個人は、その発生しうるリスクを受け入れた上で、オンラインサービスやアプリの利用習慣を意識的にコントロールし、ポジティブに利用されるデジタルフットプリントのみが残る努力を継続する。
- 企業は、社員（個人）が利用するオンラインサービスやアプリを利用して、さまざまな場に残す可能性のあるデジタルフットプリントを把握し、それが企業および個人に与えるリスクを理解すること。

（了）