企業情報をモニタリングする

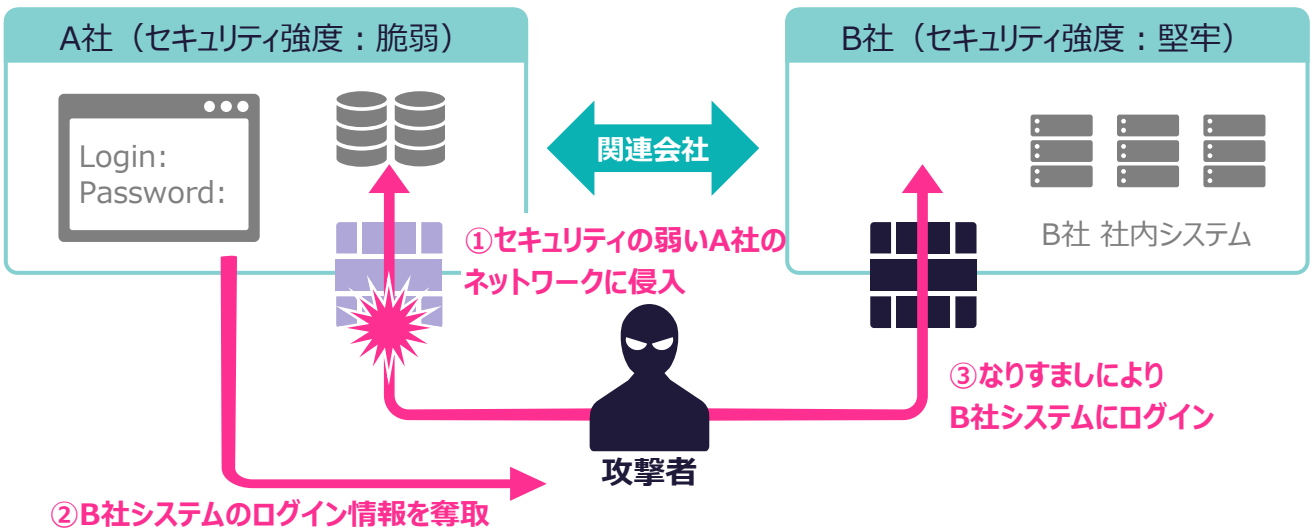
OSINT 調査『Discovery』

攻撃者に狙われるサプライチェーン

IPA の公開する「情報セキュリティ 10 大脅威 2024」において**「サプライチェーンの弱点を悪用した被害」**は 2 位にランクインしており、6 年連続 6 回目の選出になっています。さまざまな規模の企業が存在するサプライチェーンにおいて、大企業と中小企業では**セキュリティ対策への投資にギャップ**があることがしばしば見受けられます。
攻撃者であるハッカーは、攻撃が成立する確率の高い、**セキュリティ対策が手薄な中小企業**への侵入を試みます。

順位	組織向け脅威
1	ランサムウェアによる被害
2	サプライチェーンの弱点を悪用した被害
3	内部不正による情報漏えい等の被害
4	標的型攻撃による機密情報の窃取
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）

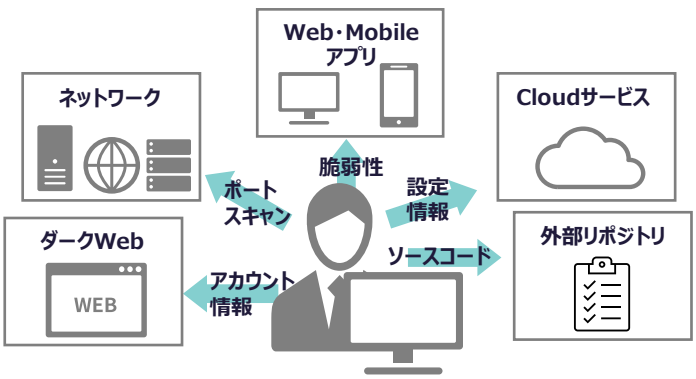
サプライチェーンのネットワークを利用した攻撃



ハッカーは、直接侵入が難しいセキュリティの強固なターゲット組織に対し、**比較的セキュリティ対策が手薄な取引先や子会社（＝サプライチェーンの弱点）などを経由**することで、ターゲット組織へと侵入します。つまり、自社のセキュリティ対策が不十分であることは、関係会社のセキュリティを脆弱な状態にしてしまうことに繋がります。セキュリティ対策は自社のみの問題ではなく、対外的にも重要な要素になっています。

公開情報による情報収集

ハッカーは、公開されている様々な情報を収集し攻撃の準備をします。公開情報には、ホームページやSNSアカウントなどの容易にアクセスができるものから、ダークWebで取引されている**「実際の攻撃手法」**や**「正規のユーザ情報」**なども含まれます。
意図していない情報の公開や、漏えいしているユーザ情報などは、**設定の変更**等で対策可能な



ものもあります。企業の中に存在する「攻撃者を侵入しやすくさせてしまう隙」を潰しておかなければ、攻撃者から目を付けられやすい状況が続き、いずれは攻撃の餌食となってしまいます。各種公開情報の把握とそれらへの対策は急務です。

企業情報モニタリング Discovery とは？

AI テクノロジーを活用した OSINT 技術に加え、エンジニアによるハッカー視点での、ダーク Web への漏えい情報を含む外部公開情報の収集・調査を行う独自の監視サービスです。

インシデントの監視および報告

セキュリティインシデントの持続的監視で、タイムリーに対応

- 盗まれた資格情報
- 公開された社内ドキュメント
- 漏洩したソースコード　　など

コンプライアンスの準拠と脆弱性予測

本番環境に害を与えない安全な外部スキャンと脆弱性予測

- Web サイトのセキュリティ
- 期限切れのドメインと証明書
- PCIDSS 準拠状況　　など

外部からの攻撃対象を予測

ハッカー目線で外部からの攻撃対象領域を監視

- API と Web サービス
- 保有する Web サイト
- ドメインと SSL 証明書　など

本調査を行う前に、リスクの高い脆弱性の有無や情報漏洩の可能性の有無を簡易的に診断することが可能です。PoC の結果をもとにして本調査の実施をご検討いただけます。

簡易調査（PoC） 100万円	本調査 個別見積
内容：簡易レポート、情報漏洩の発生有無の調査、脆弱性診断（Critical、High）	内容：詳細レポート、情報漏洩の詳細情報報告、脆弱性診断（Critical、High、Medium）

レポートサンプル　（抜粋 / 数値および内容はサンプルです）

簡易調査

本調査

IBC
アイビーシー株式会社

本社
〒104-0033
東京都中央区新川1-8-8 アクロス新川ビル8F
tel.03-5117-2780　fax.03-5117-2781

西日本事業所
〒532-0003
大阪府大阪市淀川区宮原4-1-14 住友生命新大阪北ビル3F
tel.06-7653-1014　fax. 06-7177-0542