アンラボ・セキュリティレター

Press Ahn

2023.1 Vol.109

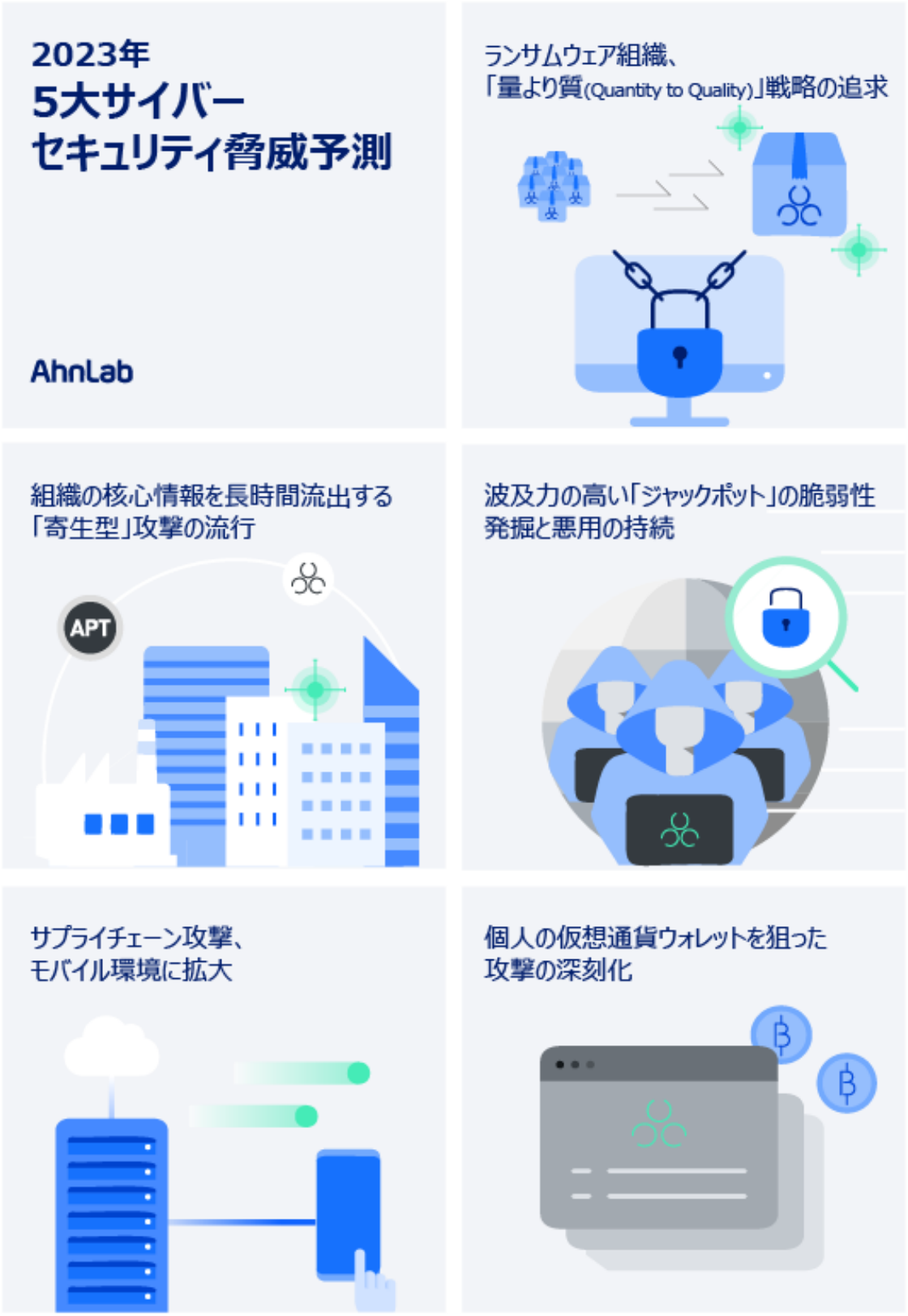
アンラボ、「2023 年 5 大サイバーセキュリティ脅威予測」を発表

アンラボ、「2023 年 5 大サイバーセキュリティ脅威予測」を発表

アンラボ (代表カン・ソッキュン、www.ahnlab.com) が 2023年に予想されるサイバーセキュリティ脅威予測をまとめ、「2023年 5大サイバーセキュリティ脅威予測」を発表した。

アンラボが予測する来年の主なセキュリティ脅威は ▲ランサムウェア組織、「量より質 (Quantity to Quality) 」戦略の追求 ▲組織の核心情報を長時間流出する「寄生型」攻撃の流行 ▲波及力の高い「ジャックポット」の脆弱性発掘と悪用の持続 ▲サプライチェーン攻撃、モバイル環境に拡大 ▲個人の仮想通貨ウォレットを狙った攻撃の深刻化などである。

アンラボセキュリティ対応センター (ASEC) のキム・ゴンウセンター長は「社会全般にわたるデジタル化によりセキュリティはもはや特定の主体だけの問題ではない」とし、「今後も攻撃者は効果を拡大化するため、すべての攻撃ポイントを活用することが予想される。そのため、一つの『完璧なセキュリティキー』を見つけるより組織とユーザーの多面的アプローチが必要な時期」と述べた。



[2023年 5大サイバーセキュリティ脅威予測]

1. ランサムウェア組織、「量より質（Quantity to Quality）」戦略の追求

最近、新規ランサムウェアの登場は停滞している中、今後、ランサムウェア攻撃グループは、最小の攻撃で最大の収益と効果を狙う「量より質」戦略を追求するものと見られる。このために攻撃グループは、まず組織の核心インフラを掌握した後、情報流出、ランサムウェア感染、DDoS まで結合する「多重脅迫」で一つのターゲットを執拗に狙うものと予測される。また、全世界的にランサムウェア組織に対する捜査と検挙が続く中、圧迫を受けたサイバー犯罪者たちが大規模攻撃を敢行した後に引退する可能性もある。したがって、組織では基本的なセキュリティシステムの構築のほか、TI（脅威インテリジェンス）を活用し、最新の攻撃動向と脆弱性情報を把握しなければならない。

2. 組織の核心情報を長時間流出する「寄生型」攻撃の流行

今年は技術や個人情報など重要資産を持つ仮想通貨取引所、大企業、公共機関などを狙った攻撃が続き、一部の攻撃グループは自分たちの成果を外部に公開したりもした。攻撃者も「投資対効果」を重要視するため、来年も主要機関や企業の核心技術および資産を窃取するための試みは続くだろうが、その方法はさらに陰密になり高度化するものと見られる。特に、過去に行ったシステムの破壊や公開といった「見せつけ」攻撃より、インフラを掌握した後、長期間にわたって核心技術や敏感情報を流出する「寄生型」攻撃が主となることが予想される。攻撃方法もアカウント情報の収集はもちろん、画面キャプチャ、映像録画や音声録音など、広範囲に拡大する可能性があり、組織はシステムのあらゆる領域を網羅して対応できる統合セキュリティシステムを構築しなければならない。

3. 波及力の高い「ジャックポット」の脆弱性発掘と悪用の持続

今年はシステムの主要権限へ正常にアクセスできるが、脆弱性を有しているドライバ（*）を悪用する「BYOVD（Bring Your Own Vulnerable Driver）」攻撃手法が発見された経緯がある。来年も攻撃者は PC からモバイル、クラウド、OT（運用・制御技術）環境などを選ばず、波及力の高い「ジャックポット」の脆弱性を見つけて攻撃に悪用する見通しである。特に攻撃者は、セキュリティパッチのサポートが切れた SW や、まだパッチが適用されていない脆弱性を直接発掘したり、ダークウェブなどで購入して、情報流出やランサムウェア攻撃に悪用する可能性がある。そのため、組織セキュリティ担当者とそのメンバーは定期的にセキュリティパッチを適用し、未使用のプログラムは削除する必要がある。

*ドライバ *(Driver):* ハードウェアデバイスと *OS* が通信できるようにするソフトウェア構成要素。*ex)* プリンター使用のための「プリンタードライバ」

4. サプライチェーン攻撃、モバイル環境に拡大

最近、金銭取引や個人情報活用などがモバイルで活発に行われる中、来年はこれまで PC 用 SW 中心に行われていたサプライチェーン攻撃（*）がモバイル分野に拡大する可能性がある。攻撃者は不正アプリ（マルウェア）を作って流布する従来の方法より、最初から通常のアプリマーケットにアプリを登録できる制作会社や制作ツールをハッキングし、アプリ制作の初期段階から侵入を試みるものと見られる。この他にもモバイルアプリの配布またはアップデート段階でマルウェアの注入を試みたり、正常モバイルアプリの認証書を窃取してこれを不正アプリ制作と配布に活用することもできる。したがって、モバイルサービス提供者であれば、開発および配布の過程で必ずセキュリティを考慮し、重要資産に対する脅威検知および対応システムを整えなければならない。

* サプライチェーン攻撃: ユーザーの多いソフトウェアの開発および配布過程に介入してマルウェアを挿入、流布する攻撃

5. 個人の仮想通貨ウォレットを狙った攻撃の深刻化

最近、大型仮想通貨取引所や主要ブロックチェーンサービスに対するハッキング攻撃が発生し、仮想通貨・NFT など仮想通貨を個人のウォレットに移すユーザーが増加している。これにより、来年は個人の仮想通貨ウォレットを狙った攻撃の試みも増加すると予想される。例えば、多くのユーザーがアカウント所有権認証およびウォレットの復旧に使用するシードフレーズ (*) や 12個 (または 24個) の単語から成り立つニーモニックキー (*) を覚えられないため、写真またはメール、携帯メモ機能などで記録する。攻撃者はこのようなニーモニックキー情報とウォレットアカウント情報を窃取するために、情報流出マルウェアや有名仮想通貨ウォレットを詐称したフィッシング Web サイト/アプリの流布を拡大するものと予想される。個人ウォレットのユーザーはシードフレーズやニーモニックキーを安全な場所に保管し、キー紛失の危険性がほとんどない安全なウォレットを使用しなければならない。また、送金しようとするウォレットの犯罪関与なども慎重に確認しなければならない。

*シードフレーズ: アカウントの所有権を認証し、ウォレットを復旧するために使用されるランダムな単語の組み合わせ

*ニーモニックキー例: desk / beach / spider / hamster / pie…

このようなセキュリティ脅威を防止するために、組織レベルでは △組織内の PC・OS・SW・Web サイトなどに対する随時セキュリティ点検およびパッチ適用 △セキュリティソリューション・サービス活用および内部社員へのセキュリティ教育実施 △管理者アカウントに対する認証履歴のモニタリング △マルチファクタ認証 (Multi-Factor Authentication) 導入などの予防対応策を講じなければならない。

また、個人は △ソース不明のメール内にある添付ファイル・URLの実行を自重 △コンテンツ・SW ダウンロードは公式経路利用 △SW・OS・インターネットブラウザなど最新のセキュリティパッチ適用 △ログイン時のパスワードの他に二重認証使用 △ワクチンの最新版維持およびリアルタイム監視機能実行など、セキュリティルールを守らなければならない。

http://jp.ahnlab.com/site/main.do
http://global.ahnlab.com/site/main.do
http://www.ahnlab.com/kr/site/main.do

アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。
1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。
アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

AhnLab

〒108-0014 東京都港区芝4丁目13- 2 田町フロントビル3階 | TEL: 03-6453-8315（代）