protiviti®
Global Business Consulting

医療分野で深刻化する高度なBad USB攻撃の脅威

スリバスタバ・パース(プロティビティ LLC シニアマネージャ)著

Bad USBとは何か?

Bad USBとは、通常のUSBフラッシュドライブを装った悪意のあるデバイスです。従来のストレージデバイスとして機能する代わりに、キーボードやマウスといったヒューマンインターフェースデバイス(HID)として動作します。これにより、USBストレージの利用制限を回避し、ユーザーの許可を得ることなく、接続されたシステム上で不正なコマンドを実行することが可能になります。

従来のBad USB攻撃は、キー入力の自動実行(キーストロークインジェクション)、マルウェアのインストール、認証情報の窃取、そしてシステムの制御奪取といった操作を数秒以内に行うために、長年にわたり利用されてきました。しかしながら、現在ではさらに進化した新型のBad USBが登場しており、その危険性は格段に高まっています。この新型Bad USBはWi-Fiモジュールを内蔵しているため、攻撃者は侵害したシステムに対し、リアルタイムでの遠隔操作や持続的なアクセスを確立することが可能になりました。

医療機関のように、医療機器、患者データ、院内ネットワークが相互接続された環境において、このような進化したBad USBを利用した攻撃が行われた場合、情報漏洩やランサムウェア感染、さらには重要な医療行為の中断といった深刻な事態を引き起こす可能性があります。

医療現場におけるUSBの主な利用場面とその悪用手口

現在のネットワーク化された環境においても、USBデバイスは依然として医療機関全体で様々な正当な目的のために広く活用されています。しかし、残念ながら、このような日常的な利用が、攻撃者にとって重要なシステムにBad USBを侵入させる好機となっています。以下に、代表的なケースを挙げます。

医療機器の保守・更新を行うベンダー技術者

MRI装置や心電図モニターなどの定期保守作業やファームウェア更新のために、医療機器の技術者が病院を訪問するケースを考えてみましょう。その際、更新作業の一環として、ベンダーが新しいファームウェアパッチを格納したUSBデバイスを使用します。

悪用手口:攻撃者は、事前にベンダーのUSBデバイスに細工をするか、あるいはベンダー担当者になりすまし、Bad USBを医療機器に接続します。これにより、わずか数秒で医療機器本体、さらにはそれが接続されている院内ネットワークにまでマルウェアが展開される恐れがあります。

病院ロビーの患者向け受付キオスク端末

最近の多くの病院では、患者が予約確認や問診票の記入などを行うためのセルフサービス式キオスク端末が導入されています。これらの端末には、保守作業を目的として、USBポートが外部からアクセス可能な状態で設置されていることがあります。

悪用手口:「心配そうな患者」や見舞客などを装った攻撃者が、監視の目が届きにくいキオスク端末のUSBポートにBad USBデバイスを短時間で接続します。マルウェアはキオスク端末のバックエンドシステムに潜り込み、そこを踏み台として、機密性の高い患者記録が保管されている内部ネットワークへと侵入を試みます。

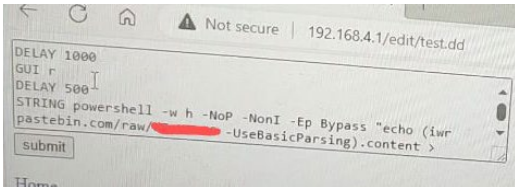
高度なBad USB攻撃の仕組み

新型Bad USBは、Wi-Fiチップを内蔵することにより、従来のモデルとは異なる動作をします。これにより、攻撃者の能力は大幅に強化されます。その仕組みは以下の通りです。

1. **周辺機器への偽装** — Bad USB は、コンピュータや医療機器に接続されると、ストレージデバイスではなくキーボードやマウスとして認識されます。これにより、従来の USB 利用制限を回避できます。

2. **Wi-Fi ネットワークの起動** — USB 内部に組み込まれたチップが不正な Wi-Fi ネットワークを生成し、攻撃者はこれに遠隔から接続します。

3. **リモートでのコマンド実行** — 接続後、攻撃者は無制限にスクリプトを実行できます。これは、挿入時に単一のスクリプトしか実行できなかった従来の Bad USB とは異なる点です。



4. **システムの侵害** — リアルタイム制御により、攻撃者はマルウェアの展開、患者データの窃取、医療システムの無効化、さらには接続された IoT 医療機器の操作まで行うことが可能です。

5. **持続性と潜伏性** — 初期ペイロードの実行に失敗した場合でも、攻撃者は物理的にその場にいることなく、スクリプトの再実行、セキュリティ対策の回避、そして侵害したマシンへの持続的なアクセスを維持できます。

高度な Bad USB 攻撃が医療分野において特に危険な理由

医療業界は、患者データの価値の高さと医療システムの重要性から、サイバー犯罪者にとって主要な標的となっています。高度な Bad USB 攻撃は、以下のような事態を引き起こす可能性があります。

1. **患者データへの不正アクセス**

- 電子カルテ（EHR）には、個人の機密情報や医療情報が含まれており、これらはダークウェブで売買されたり、個人情報の盗難に悪用されたりする可能性があります。
- 攻撃者は、悪意のある USB を接続してから数秒以内に患者データを窃取することが可能です。

2. **病院ネットワークへのランサムウェア展開**

- リアルタイムでのリモートアクセスにより、攻撃者は病院システムにランサムウェアを注入し、患者記録を暗号化してアクセス復旧のために身代金を要求することができます。
- これは、治療の遅延、誤診、さらには人命に関わる事態につながる可能性があります。

3. **医療機器の侵害**

- 輸液ポンプ、人工呼吸器、画像診断システムなど、多くの医療機器は病院のネットワークに接続されています。
- 攻撃者は、これらの機器の設定を遠隔から操作し、機器の故障を誘発したり、投薬量を誤らせたりする可能性があります。

4. **重要な医療業務の阻害**

- 攻撃者はマルウェアを展開して、病院管理システムをクラッシュさせたり、通信チャネルを混乱させたり、救急医療サービスを停止させたりする可能性があります。
- 広範囲な攻撃が発生した場合、部門全体の機能の停止、手術の延期や医療危機的状況を招く恐れがあります。

医療機関における高度な Bad USB 攻撃への対策

このような巧妙な攻撃のリスクを軽減するため、病院および医療機関は多層的なサイバーセキュリティアプローチを採用する必要があります。

1. **USB および周辺機器のアクセス制限**

- エンドポイントセキュリティソリューションを使用し、未承認の HID デバイス（キーボード、マウス、またはその他の入力デバイス）の接続をブロックする。
- 厳格な USB ポリシーを導入し、承認された医療機器および暗号化されたストレージデバイスのみ使用を許可する。

- 不正なHIDベースのUSB攻撃を検知・ブロックできるUSBポートセキュリティソリューションを利用する。

2. **ワイヤレス活動および不正 Wi-Fi ネットワークの監視**

- Wi-Fiスキャンソリューションを導入し、不正なアクセスポイントを検知する。
- 院内に未知のWi-Fiネットワークが出現した場合にセキュリティチームに警告するよう、ネットワークモニタリングツールを設定する。
- 院内端末における未知のWi-Fiネットワークへの自動接続を無効にする。

3. **USB を介した脅威に関する医療スタッフへの教育訓練**

- 医療用コンピュータや院内ネットワークに未知のUSBデバイスを接続する危険性について、職員を教育する。
- 業務用端末での私物USBドライブの使用を禁止する厳格なポリシーを導入する。
- 模擬的なフィッシング訓練やUSB攻撃演習を実施し、職員の意識を向上させる。

4. **エンドポイント検知・対応（EDR）ソリューションの導入**

- 振る舞い検知型セキュリティソリューションを導入し、偽装HIDデバイスからのキーストロークインジェクション攻撃を監視する。
- 接続デバイスのリアルタイムモニタリングを徹底し、不審な挙動を警告する。
- 感染したシステムを隔離し、横展開(ラテラルムーブメント)を防ぐための自動対応策を導入する。

5. **ゼロトラストセキュリティアーキテクチャの導入**

- 院内ネットワークへのアクセスを許可する前に、全てのデバイスとユーザーを検証するゼロトラストのアプローチを採用する。
- 全ての特権アカウントに対して多要素認証（MFA）を必須とする。
- 不正なスクリプト実行を防ぐため、権限昇格を制限する。

6. **定期的なセキュリティ監査とテストの実施**

- ペネトレーションテストを実施し、院内システムの脆弱性を評価する。
- Bad USB攻撃をシミュレートするレッドチーム演習を実施し、インシデント対応チームを訓練する。
- データ保護戦略を強化するため、サイバーセキュリティ関連のコンプライアンス(例：HIPAA、GDPR)の遵守を徹底する。

結論

医療機関において業務のデジタル化が進むにつれて、サイバー犯罪者は医療システムの脆弱性を悪用するための手口を進化させています。Wi-Fi機能を内蔵した新世代のBad USBデバイスは、重大な脅威となります。これにより攻撃者は、リモートアクセス、無制限のスクリプト実行、そして病院ネットワークを数秒以内に侵害する能力を手に入れます。

これらのデバイスはキーボードやマウスとして偽装するため、たとえ従来のUSB制限をもってしても、その実行を完全に防ぐことはできません。医療機関は、基本的なUSBブロッキングにとどまらず、これらの隠れた脅威から防御するため、より厳格なセキュリティ対策を講じる必要があります。

USBおよびHIDデバイスの制限、ワイヤレスアクティビティの監視、ならびにサイバーセキュリティのベストプラクティスに関するスタッフ教育やトレーニングを実施することにより、医療機関はこれらの高度な攻撃のリスクを軽減し、患者の安全が損なわれないようにすることができます。

プロティビティについて

プロティビティは、企業のリーダーが自信をもって未来に立ち向かうために、高い専門性と客観性のある洞察力や、お客様ごとに的確なアプローチを提供し、ゆるぎない最善の連携を約束するグローバルコンサルティングファームです。25ヶ国、90を超える拠点で、プロティビティとそのメンバーファームはクライアントに、ガバナンス、リスク、内部監査、経理財務、テクノロジー、デジタル、オペレーション、人材・組織、データ分析におけるコンサルティングサービスを提供しています。プロティビティは、米国フォーチュン誌の働きがいのある会社ベスト100に10年連続で選出され、Fortune 100の80%以上、Fortune 500の約80%の企業にサービスを提供しています。また、成長著しい中小企業や、上場を目指している企業、政府機関等も支援しています。プロティビティはRobert Half（RHI）の100%子会社です。

© 2025 Protiviti Inc. All rights reserved. 複写禁、転載禁

protiviti®