無線LANを狙う 11のセキュリティの脅威

無線LANの利便性が認知され、さまざまな場所での利用が急増するにつれ、無線LANに関連する脆弱性を悪用した無差別のセキュリティ犯罪や標的型攻撃が増加しています。商業的、政治的、または社会的などのさまざまな動機を持つ洗練されたサイバー犯罪者が、攻撃の機会をうかがっています。無線LANを正しく管理しない場合には、顧客や取引先、社内ユーザなどの機密情報を外部に公開してしまうリスクが発生します。ここでは、無線LAN環境を狙う11のセキュリティの脅威を解説します。

1 Wi-Fi パスワードクラック

WEPなどの古いセキュリティプロトコルがいまだに使用されている無線アクセスポイントは、パスワードを簡単に解読できてしまうため、簡単に標的にされてしまいます。

2 不正APとクライアント

サイバー犯罪者がホットスポットの近くで偽装したSSIDのアクセスポイントを用意すれば、ユーザは疑うことなく簡単にログインしてしまうでしょう。そして、不正APによる不正コードインジェクションの被害者となってしまったことに気付くユーザーは少ないでしょう。

3 マルウェアの拡散

ゲスト用の無線ネットワークの利用者は、近くにいる悪意あるユーザーが送り込むマルウェアの影響を知らぬ間に受けることになります。ハッカーが良く使う方法の1つに、バックドアを仕込んで後から機密情報を盗むという手口があります。

4 盗聴

セキュリティ対策が不十分なネットワークを悪用して私的なやり取りを盗聴されたり、パケットを傍受されたりする恐れがあります。

5 データの不正取得

ユーザーは、無防備な無線ネットワークにアクセスした瞬間から、極秘情報が含まれる私的文書がネットワーク経由で送受信されたり、データが傍受されサイバー犯罪者の手に渡るリスクにさらされます。

6 不正・違法使用

ゲスト用のWi-Fiが違法性や有害性の疑われる通信に悪用されるリスクがあります。成人向けや過激なコンテンツは周りのユーザーに不快感を与える恐れがあり、著作権で保護されたメディアの違法ダウンロードは著作権侵害の訴訟に発展する可能性があります。

7 悪意ある近隣ユーザ

無線LANネットワーク上のユーザ数が増えれば、マルウェアに感染した端末が同一ネットワーク上で活動している可能性も高くなります。AndroidのStagefrightなどのモバイル攻撃では、被害が表面下する前にゲスト間での感染が広がっていることもあります。

8 中間者攻撃（MIM）

無線LAN経由の日常的なやり取りでも、犯罪者が密かに傍受して、正規の違法性のない内容が書き換えられてしまうことで、データ流出につながることがあります。

9 無線LANに対するDoS攻撃

攻撃者が正規のアクセスポイントに意図的に大量のトラフィックを送信し、アプライアンスを使用できなくすることで、正規ユーザがWi-Fiにアクセスできなくするものです。

10 なりすまし攻撃

Wi-Fiのセキュリティを攻撃するサイバー犯罪者は一般的に、MACアドレスを偽装することで正規あるいは既知のデバイスであるかのように装います。

11 APの構成ミス

ワイヤレスセキュリティのベストプラクティスに従わずにアクセスポイントを導入すると、構成ミスによって、セキュリティリスクにさらされる危険性が高まります。

無線LANの構築は容易ですが、そのセキュリティ対策は多くの課題を抱えています。
WatchGuardは、WIPS（特許取得:ワイヤレス侵入防止システム）で強固なセキュリティ機能を提供します。
ぜひお問合せください。

Learn More at: www.watchguard.co.jp

WatchGuard®