WatchGuard

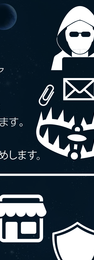
2016 セキュリティ動向予測

セキュリティ脅威の形態は常に変化し、サイバー犯罪者は新旧さまざまな方法でその範囲を拡大しながら、ユーザを騙して価値あるデータを盗み取ろうとします。確実な防御を実現するため、ウォッチガードでは、セキュリティのベストプラクティスに従うこと、脅威や標的型ソーシャルエンジニアリングの手口を含め、社員を教育すること、最新のネットワークセキュリティ技術を導入してセキュリティ上の問題を迅速に特定することを推奨します。
そうすることで、2016 年に起こると予想される攻撃にも高い確率で対抗できます。

1. Androidを標的にするランサムウェア

サイバー犯罪に狙われるプラットフォームが拡大:

ランサムウェアが拡大し、ファイルが暗号化され、実際に身代金の要求に応じてしまった事例が多く報告されています。これまでのランサムウェアの主な標的は Windows でしたが、来年は、Android のモバイルデバイスや Apple社のラップトップなどの他のプラットフォームでも動作するランサムウェアが出現するでしょう。



2. 人々を陥れる罠

ソーシャルエンジニアリングが引き続き最大の脅威に:

最近発生した高度なネットワーク攻撃による被害に共通するのは、スピアフィッシングをきっかけとする攻撃手法です。サイバー攻撃では、ソーシャルエンジニアリングを悪用し、特定のユーザ向けにコンタクトをカスタマイズすることで相手を信用させ、情報を搾取する手法が使われます。社員を対象とするセキュリティ関連のトレーニングを実施して、最新のソーシャルエンジニアリングを悪用する攻撃手法を学習することをお勧めします。

3. 古いタイプの攻撃が今後も継続

基本的セキュリティ対策の重要性:

大多数のセキュリティ攻撃、特に中堅・中小企業に対する攻撃は依然として旧来の基本的な手法に依存しています。洗練された巧妙なテクニックによる攻撃が増加する一方、中堅・中小企業でのセキュリティのインシデントは依然として基本的なセキュリティ対策の不足が要因として発生しています。まずは基本的なセキュリティ対策を見直すことで、2016年に発生するセキュリティの攻撃によるリスクを軽減する事が可能です。

4. iOSを狙う攻撃の増加

iOS を標的にしたマルウェアの襲来:

Googleのオープンプラットフォーム戦略により、Apple社iOSデバイスよりもアンドロイドデバイスの方がより脅威のリスクが増加していると思われています。昨年、攻撃者はApple社の開発プラットフォームへの感染に成功しました。
攻撃者は、今後も継続してApple社マーケットプレイス上にマルウェアを感染を試みると思われます。 iOSデバイオスをターゲットとされた攻撃が始まります。

5. 悪意ある広告、マルバタイジングの増加

暗号化を悪用したマルバタイジングの増加:

マルウェアとアドバタイジング(広告)を組み合わせた造語であるマルバタイジング(悪意ある広告)は、アドバタイジングネットワークとして信頼されている Web サイトに悪意あるコードを送り込むことで正規であるかのように装う攻撃です。一部のサービスや製品は、悪質なマルウェアを含む広告の検知性能を向上させている一方で、攻撃者もさらに新たな手法を使用しています。
2016年は、マルバタイジングが 3倍に増え、HTTPS の使用が拡大することでマルバタイジングによる攻撃が増加することが予想されます。

6. 人工知能と機械学習の活用

自動化による次のレベルのセキュリティ対策:

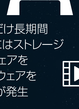
今日の自動化された攻撃は常にリアクション型の防御を回避します。シグネチャベースのセキュリティ対策は、もはや有効ではありません。人的リソースによる 監視により、新たな脅威を識別することは可能ですが、サイバー犯罪者は、セキュリティ監視に人的リソースが追いついていないことを既に理解しています。
一体、どのように対抗すれば良いのでしょうか。悪意ある挙動を自動認識できる人工知能(AI)と機械学習が解決の鍵となるでしょう。

7. 教育団体を標的にした攻撃

学生のデータを狙うサイバー犯罪が増加:

情報セキュリティとは、究極的にはデータを保護することであり、個人を完全に特定できるデータである個人情報は、特に価値の高い情報であると言えます。学生である間、大量のデータが収集されますが、その中には、最も価値ある個人情報である医療情報も含まれます。
これらの情報が教育機関のオープンネットワーク環境に置かれていることから、2016年は学生のデータを狙うサイバー犯罪が増加すると予想されます。教育機関の個人情報を管理する担当者は、学生のデータに関連するデータベースセキュリティを強化し、Web アプリケーションを再検証する必要があります。

8. IoT に対する攻撃



モノのインターネット(IoT)のファームウェアが攻撃:

コンピュータの乗っ取りを企むハッカーは、悪意あるコードをできるだけ長期間デバイスに常駐させようとします。しかし、ほとんどの IoT デバイスにはストレージがなく、リソースもわずかであるため、コードを送り込んでファームウェアを書き換える方法が使われるでしょう。来年はIoT デバイスのファームウェアを書き換えてデバイスを乗っ取る、POC (proof-of-concept)型攻撃が発生すると予想しています。
対抗策として、ベンダーも デバイスのファームウェア書き換えを困難にするセキュアブートのメカニズムを実装し、セキュリティの強化を図るようになるでしょう。

9. ワイヤレス環境への侵入

ワイヤレスの「簡単接続」が深刻な脆弱性に:

ワイヤレス環境では今後、「簡単接続」の機能に関する深刻な脆弱性が見つかると予想されます。たとえば、WPS(Wi-Fi Protected Setup)を使用すれば、新規ユーザーが複雑なパスワードを入力することなく、簡単にセキュアワイヤレスネットワークに参加できます。しかし、この機能により、攻撃者にもワイヤレスネットワークの侵入を簡単に許してしまうという脆弱性があります。
ワイヤレスネットワーク関連でこれから見つかる脆弱性は、ネットワークへの容易な参加を実現する機能と関連性のあるものになるでしょう。

10. 報道サイトを狙う大掛かりな攻撃

ハクティビストによる報道サイトのハッキング:

人目につかずに悪巧みをするサイバー犯罪者とは異なり、ハクティビストは、大げさなメッセージを大々的に発表して注目を集めたいと考えています。ハクティビストによるサイバー活動の本質は、最も効果的な方法と場所を使って、できる だけ多くの人にメッセージが伝わるようにすることにあります。有名なビデオを数多く公開しているアノニマスが、その代表的な例です。来年は、ハクティビストによる全世界に向けた大掛かりなライブ映像が公開されると予測されます。

セキュリティ情報は ウォッチガード セキュリティセンター:

www.watchguard.co.jp/Security-center

WatchGuard