Q4 2016 インターネットセキュリティレポート

WatchGuard 脅威ラボによるインターネットセキュリティレポート

2016年Q4（10月～12月)は、情報セキュリティに関して、新たな傾向を示す期間でした。ビジネスを保護する活動を開始する前に、最新の脅威の状況を把握する必要があります。WatchGuard 脅威ラボの脅威分析チームは、ユーザに役立つインターネットセキュリティレポートを四半期毎に提供します。

最新の攻撃手法

マクロベースのマルウェアは継続的に猛威を発揮!

古い技法であるにもかかわらず、多くのスピアフィッシングによる攻撃には、悪意あるマクロを含む文書が含まれており、依然として、効力を持っています。

Javascriptを悪用する攻撃が依然として流行!

Javascriptは、メールやウェブを介在してマルウェアの配信と難読化の仕組みを持つマルウェアとして、攻撃者に継続して利用されています。

日々報告されるゼロデイの脅威!

30%のマルウェアは「ゼロデイの脅威」として、従来のウイルス対策ソリューションでは検知できません。高度な保護ソリューションがなければ、3分の1の脅威が見逃されています。

30%

Webサイトは戦場

10 OUT OF 10

ほとんどの攻撃はWebベースでの攻撃

73%

のWebベースの攻撃は、ドライブバイダウンロード攻撃のために、ブラウザをターゲットに。

エクスプロイトキットは、攻撃者にとって、マルウェアを配信する一般的な方法として、悪質なJavaScriptの蔓延を助長

脅威のトレンド

銀行が標的に!

洗練された攻撃者は、回避型のマルウェアを利用して銀行を標的とした攻撃を続けています。

IoTへのトロイの木馬攻撃

Linuxベースのトロイの木馬が急増し、IoTへの攻撃に繋がっています。

国家レベルでのハッキング

国家組織を狙うハッカーは、犯罪者と同様のハッキングツールを使用しますが、より洗練された難読化および回避技術を使用します。

WatchGuard の実績

3.04M（300万件以上）

ウォッチガードによってブロックしたネットワーク攻撃（Q4 2016）

123 件

1デバイスあたりの攻撃数

18.7M（1、800万件以上）

ウォッチガードによってマルウェアの亜種をブロック

758 件

1デバイスが検出したマルウェアの種類

インターネットセキュリティレポートの詳細版は以下よりご確認下さい。

www.watchguard.co.jp/security-news

WatchGuard