サイバー攻撃の傾向として、ログイン情報の盗難が顕著に

ウォッチガードの2017年第2四半期のインターネットセキュリティレポートでは、マルウェアの47%が
未知またはゼロデイマルウェアであると報告、WannyCryの包括分析も提供

2017年11月9日（木）
ー企業向け統合型セキュリティプラットフォームのグローバルリーダであるWatchGuard（R）Technologiesの日本法人、ウォッチガード・テクノロジー・ジャパン株式会社（本社：東京都港区、社長執行役員
根岸正人、以下ウォッチガード）は、四半期毎に作成している「インターネットセキュリティレポート
日本語版」を発表しました。本レポートでは、中堅・中小企業（SMB）および分散拠点を持つ大企業を対象とした、コンピュータ並びにネットワークセキュリティの脅威に関する最新情報を提供しています。2017年第2四半期では、ユーザのログイン情報の不正取得を試みる犯罪手法の著しい増加が見られ、未知あるいはゼロデイのマルウェアが47%に達しており、シグニチャベースのアンチウイルスソリューションでは対応しきれなくなっていると報告しています。

ウォッチガードのCTO（チーフテクノロジオフィサー）であるコリー・ナクライナー（Corey Nachreiner）は、次のように説明しています。「第2四半期の間に収集されたFireboxのデータから、これまで以上にログイン情報の詐取を目的とした脅威が高まっていることが読み取れます。JavaScriptを悪用したフィッシング攻撃、Linuxパスワードの盗難攻撃、さらにWebサーバに対するブルートフォース攻撃など、犯罪の主流がログインアクセスに移行していることが明らかになっています。つまり、企業は無防備なサーバを堅牢にし、多要素認証の導入を真剣に考え、フィッシング攻撃を特定できるようにユーザを教育し、貴重なデータを保護するための標的型攻撃対策ソリューションを導入すべきだと言えます。」

ウォッチガードのインターネットセキュリティレポートでは、脅威インテリジェンス、調査結果、並びにセキュリティのベストプラクティスを報告しており、読者自身および所属する組織を守るためにオンライン攻撃に関する知見の提供と啓蒙活動を目的としています。2017年第2四半期のレポートの主な調査結果を以下に紹介します：

・
Mimikatzがマルウェアのトップランキングで36%を占めています。Mimikatzは、ログイン情報の詐取を目的とした幅広く利用されているオープンソースツールであり、本四半期において初めてマルウェアのトップ10に名を連ねました。Mimikatzは、一般的にWindowsのログイン情報の盗難およびリプレースに使用され、頻繁に利用されたことから第2四半期のマルウェアのトップランキングに登場しました。今回これまでにないマルウェアが登場してきたことは、攻撃者が常に攻撃手法を変えてきていることを示唆しています。

・
ユーザを騙すために、フィッシング攻撃に悪意のあるJavaScriptが利用されています。ここ最近

の四半期では、Webおよびメールベースの攻撃の両方においてマルウェアを潜入させるために、攻撃者はJavaScriptのコードおよびダウンローダーを使用してきました。第2四半期では、攻撃者はフィッシングメールにおいてHTMLの添付ファイルにJavaScriptを使用し、Google、Microsoft、および他の著名な正規サイトのログインページを模倣することでユーザのログイン情報を詐取してきました。

・
北欧ではLinuxのパスワードが攻撃者の大きな標的となりました。サイバー犯罪者は、旧来のLinuxアプリケーションの脆弱性を利用し、北欧諸国およびオランダを攻撃対象としてパスワードのハッシュファイルの盗難を試みています。攻撃の75%以上が/etc/passwdファイルへのアクセスを目的としたリモートファイルインクルードの脆弱性を活用しており、ノルウェーで62.7%、フィンランドで14.4%を占めています。

・
Webサーバに対するブルートフォース攻撃が増加しました。今夏、ユーザのログイン情報を詐取するために、Webサーバに対する攻撃に自動化ツールが使用されました。第2四半期では認証情報に対するWebベースの攻撃が流行しましたが、Webサーバへのブルートフォースによるログイン情報の攻撃がネットワーク攻撃のトップテンに入りました。保護機能を備えていないWebサーバでは、ログインの失敗を監視しているにもかかわらず、結果として毎秒数千単位でパスワードの入力を試みる自動化攻撃に対応することができませんでした。

・
マルウェアの半数近くが既存のアンチウイルスソリューションを回避しています。新種またはゼロデイマルウェアが既存のアンチウイルスソリューションを回避する確率は47%となり、これまでになく増加しています。このデータは、新たな脅威の検知において、旧来のシグニチャベースのアンチウイルスの信頼性が著しく損なわれていることを示唆しており、標的型攻撃を検知するには振る舞い検知のソリューションが必要であることを証明しています。

ウォッチガードのインターネットセキュリティレポートは、世界中で運用されている膨大な数のセキュリティアプライアンスの一部である、33,500台以上の統合セキュリティアプライアンスから取得される匿名データを基に作成されています。第2四半期において、これらのアプライアンスは合計1,600万種以上（1デバイス平均で488種類）のマルウェアを防御しています。また、同四半期でウォッチガードのゲートウェイアンチウイルスソリューションは、1,100万種近いマルウェアを阻止しており（Q1と比較して35%増）、さらにクラウド型サンドボックスセキュリティサービス（APT Blocker）では別途5,484,320件のマルウェアを検知しています（Q1と比較して53%増）。また、WatchGuard Fireboxアプライアンスでは、第2四半期で約300万件のネットワーク攻撃を阻止しており、アプライアンス1台に換算すると平均86件の攻撃を阻止したことになります。

レポートでは、2017年第2四半期におけるトップマルウェアおよび攻撃の傾向の詳細、また、悪名高いWannaCryランサムウェア攻撃の包括的概要、そして読者向けにセキュリティのベストプラクティスに関する主要情報を掲載しています。また、ウォッチガードのThreat Lab（脅威ラボ）による最新の調査プロジェクトでは、SSHおよびTelnetにおける常時自動攻撃の標的にされるハニーポットで取得された脅威傾向にも着目しています。本プロジェクトの教訓として、デフォルトのログイン情報にまつわる危険性とIoTデバイスの保護の重要性を学び取ることができます。

レポートの全内容は以下よりダウンロードすることができます。
https://www.watchguard.co.jp/whitepaper

【WatchGuard Technologiesについて】
WatchGuard (R)
Technologiesは、業界標準ハードウェア、ベストオブブリードセキュリティ、ポリシーベースの管理ツールを独自アーキテクチャにより統合したビジネスセキュリティソリューションを提供するグローバルリーダとして、全世界の企業にエンタープライズクラスのセキュリティソリューションを提供しています。本社を米国ワシントン州シアトルに置き、北米、ヨーロッパ、アジア太平洋地区、中南米に支社を展開しています。日本法人であるウォッチガード・テクノロジー・ジャパン株式会社は、多くのパートナーを通じて、アプライアンス製品、ネットワークからエンドポイントまでの脅威検知とセキュリティの「可視化」及びセキュリティとネットワークの「運用管理」など拡大するニーズへのソリューションを提供しています。詳細は
http://www.watchguard.co.jp をご覧下さい。

さらなる詳細情報、プロモーション活動、最新動向はTwitter（@WatchGuardJapan）、facebook（@WatchGuard.jp）、をフォローして下さい。また、最新の脅威に関するリアルタイム情報やその対策法はセキュリティセンターまでアクセスして下さい。
セキュリティセンター：https://www.watchguard.co.jp/security-center

WatchGuardは、WatchGuard Technologies,
Inc.の登録商標です。その他の商標は各社に帰属します。

【本プレスリリースに関するお問合せ】
ウォッチガード・テクノロジー・ジャパン株式会社
〒106-0041
東京都港区麻布台1-11-9 BPRプレイス神谷町5階
マーケティング担当：角田・堀江
Tel： 03-5797-7205
Fax： 03-5797-7207
Email： jpnsales@watchguard.com
URL： http://www.watchguard.co.jp

Generated by ぷれりりプレスリリース
https://www.prerele.com