ウォッチガード、脆弱なパスワードによる脅威への対策に多要素認証が必要と警告

2018年第2四半期のインターネットセキュリティレポート、認証情報を標的とした攻撃と不正なOfficeドキュメントを悪用した攻撃の増加を確認

2018年9月14日（金）
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、代表執行役員社長 谷口
忠彦、以下ウォッチガード）は、中堅／中小企業（SMB）や分散拠点を持つ大企業を標的とした最新のセキュリティ脅威の調査を目的とした、四半期毎に発行している「インターネットセキュリティレポート」の最新版（2018年第2四半期）を発表しました。ウォッチガード脅威ラボの調査により、公務員および軍人のLinkedInのパスワードの約半数が、2日とかからない時間内に解明される脆弱レベルにあることが明らかになりました。こうした現実と、Webアプリケーションに対するブルートフォースログイン攻撃の脅威、認証情報を詐取する強力なマルウェア、Mimikatzの台頭などにより、もはやパスワードだけでは保護機能が十分に機能せず、組織を問わず多要素認証（MFA）ソリューションが必要であることが確認されました。

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。「2018年第2四半期ではパスワードおよび認証情報の詐取にフォーカスした脅威が多発しており、セキュリティの要である認証の重要性が益々高まっていることは確実です。認証情報を盗難する回避型のマルウェアやその亜種、ブルートフォースログイン攻撃などにより、サイバー犯罪者はパスワードのハッキングに注力しており、アクセス制限のかかったネットワークや機密データへのアクセスを目論んでいます。ウォッチガードではこうした傾向を踏まえて、クラウド型の多要素認証ソリューションWatchGuard AuthPoint、並びに従来のシグネチャベースのアンチウイルスを回避するマルウェアを阻止する3つ目のマルウェア検知エンジンとなるIntelligentAVサービスなど、革新的な防御機能を新たにポートフォリオに追加しています。すべての組織は、これらの進化し続ける攻撃手法に対抗できる多層防御機能を提供するベンダーやソリューションプロバイダを検討するべきです。」

四半期毎に作成されている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、セキュリティに対する知見、調査結果、そしてベストプラクティスを提供しており、あらゆる規模の組織に役立つ最新のサイバーセキュリティ動向、並びに組織および組織のパートナーや顧客を進化するセキュリティ脅威から身を守る方法を紹介しています。以下に2018年第2四半期レポートにおける主な調査結果を紹介します：

約半数の公務員および軍人のパスワードが脆弱であることが判明。ユーザのパスワード強度を測定するために、ウォッチガード脅威ラボがLinkedInにおける2012年のデータダンプを分析した結

果、データベース内の「.mil」および「.gov」のメールアドレスドメインに関係するパスワードの半数が客観的分析により脆弱であることが判明しました。データベース内の公務員および軍人のアカウントパスワード355,023件のうち、178,580件が2日以内に解読されました。これらのアカウントで最もよく使用されていたパスワードには「123456」、「password」、「linkedin」、「sunshine」、そして「111111」といった単純なものが含まれていました。民間人でも同程度の50%超のパスワードが脆弱なものでした。こうした結果から、すべての人にとってより強力なパスワードが必要であり、機密情報を扱う公務員はなおのこと、さらに高水準のセキュリティが求められることが明らかとなりました。パスワード設定における詳細なトレーニングや方法に加えて、すべての組織は多要素認証ソリューションを導入し、情報漏えいリスクの削減に努めるべきです。

Mimikatzが第2四半期で最も流行したマルウェア。Mimikatzは今期のトップ10マルウェア亜種の中で、27.2%を占めました。以前よりパスワードや認証情報を詐取することで有名なマルウェアでしたが、過去にトップにランクされたことはありませんでした。Mimikatzによる被害の急増は、認証攻撃や認証情報の窃取はサイバー犯罪者にとって未だに主要な攻撃対象であることが判明し、パスワード単体ではセキュリティを確保する上で不十分であるため、ネットワークアクセスに必要となる認証要素を増やすことで、ハッカーによる攻撃の難易度を上げる多要素認証（MFA）により強化すべきであることを示唆しています。

マルウェア攻撃の75%以上がWeb上で実行。第2四半期で報告された脅威の76%がWebベースであり、組織が圧倒的多数の攻撃を阻止するためには、HTTPおよびHTTPSインスペクションの仕組みを取り入れるべきであることを示唆しています。Web攻撃に特化した脅威として4位にランク付けされた「WEB Brute Force Login - 1.1021」では、攻撃者がWebアプリケーションに対して膨大な量のログイン試行を実施し、短時間でユーザのパスワードを解読するためにランダムな文字列の組み合わせを試行します。この攻撃は特に、サイバー犯罪者が認証情報の窃取に重きを置いている証拠として挙げることができ、もはや複雑で強度の高いパスワード設定だけでなく、より効果的な防止策として多要素認証（MFA）ソリューションの導入が重要であることを示しています。

仮想通貨マイニングがトップクラスのマルウェアとして報告。予測通り、悪意のある仮想通貨マイニングがハッキング手法として引き続き増加しており、第2四半期においてウォッチガードのトップ10マルウェアリストに初登場しました。ウォッチガードは前期において、「Coinhive」と呼ばれるJavaScriptの仮想通貨マイニングに匹敵し、感染被害者のコンピュータリソースを利用して仮想通貨Monero（XRM）を採掘する仮想通貨マイニングCryptominer.AYを公表しています。この調査結果では、この仮想通貨マイニングで最も被害を受けた地域は米国であり、総攻撃数の約75%を占めました。

サイバー犯罪者は引き続き不正なOfficeドキュメントを悪用。攻撃者は引き続きOfficeドキュメントに罠を仕掛けており、普及しているMicrosoft製品に潜む脆弱性を悪用して一般ユーザを欺いています。興味深いことに、3つの新たなOfficeマルウェア攻撃がウォッチガードのトップ10リストに名を連ね、これらの攻撃の75%が欧州地域を標的としており、特にドイツのユーザが狙われました。

インターネットセキュリティレポートの完全版では、EFail暗号化の脆弱性に関する詳細分析結果、および第2四半期におけるトップリストに並ぶ攻撃に対する知見、並びにSMBのセキュリティ体制の改善に役立つ防御戦略について紹介しています。調査結果は世界中で実稼働している約40,000台に及ぶウォッチガードのUTMアプライアンスFireboxの匿名データに基づいており、これらのアプライアンスは2018年第2四半期で、約1,400万件以上のマルウェア亜種を防御し（1デバイス当た

り449件）、また100万件以上のネットワーク攻撃を防御しています（1デバイス当たり26件）。

レポート全文は以下よりダウンロードできます。
https://www.watchguard.com/wgrd-resource-center/security-report
（英語）*日本語レポートは後日公開予定。

また、攻撃の種類、地域、日時ごとにリアルタイムで脅威の知見を提供するウォッチガードの脅威ランドスケープはこちらよりご覧になれます。（英語）
https://www.secplicity.org/threat-landscape/

インターネットセキュリティレポートの担当チームおよびSecplicity.orgによる最新ポッドキャストは「The 443　Security Simplified」https://www.secplicity.org/category/the-443/（英語）に是非アクセスして下さい。本ポッドキャストでは、毎週最新のハッキング、攻撃、侵害に関する手法やテクニックについて分析しています。また、最新の脅威情報、攻撃手法を紹介し、企業の防御対策に役立つ実用的な知見を提供します。

【WatchGuard Technologiesについて】
WatchGuard (R) Technologiesは、ネットワークセキュリティ、セキュアWi-Fi、多要素認証、そしてネットワークインテリジェントを提供するグローバルリーダとして、全世界で約10,000社の販売パートナーとサービスプロバイダより80,000社以上の企業にエンタープライズクラスのセキュリティ製品とサービスを提供しています。ウォッチガードのミッションは、中堅・中小企業や分散型企業を含むすべての企業がエンタープライズレベルのセキュリティをシンプルに利用できるようにすることです。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、数多くのパートナーを通じて、国内で拡大する多様なセキュリティ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SecplicityJPまでアクセスして下さい。
SecplicityJP： https://www.watchguard.co.jp/security-news

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： https://www.watchguard.co.jp

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