プレスリリース: 2016年04月22日
トピック: ソフトウェア/ ITサービス

ヒューレット　パッカード　エンタープライズ、今日の企業にとっての重大リスクを特定：アプリケーションの脆弱性、パッチ、およびマルウェアのマネタイゼーション

-　今年のサイバーリスクレポートで、攻撃の高度化が進み、企業はネットワーク境界の消滅とプラットフォーム多様化への対応に課題を抱えていると報告 -

2016年4月22日

日本ヒューレット・パッカード株式会社

本リリースは、ヒューレット　パッカード　エンタープライズ（本社：米国カリフォルニア州パロアルト、以下：HPE）が、2016年2月17日（現地時間）に米国で発表した英文リリースに基づいて作成した日本語抄訳です。

ヒューレット　パッカード　エンタープライズ（NYSE：HPE）は、「2016年版サイバーリスクレポート」を発表し、過去1年間において企業を悩ませた重大なセキュリティ脅威を明らかにしました。

従来のネットワーク境界が消滅し、攻撃対象領域が拡大するにつれ、セキュリティ専門家たちは、イノベーションの鈍化や事業スケジュールの遅延を招くことなく、ユーザー、アプリケーションおよびデータを保護する必要があります。今年のサイバーリスクレポートは、こうした動向を背景とした2015年の脅威状況を詳しく調べ、アプリケーションの脆弱性、セキュリティパッチ、マルウェアのマネタイゼーションなど主要なリスク分野を中心に対応策を提案します。また同レポートでは、セキュリティ分析の新規則や注目を集めたデータ侵害の「付随的損害」、政治課題の変化、プライバシーとセキュリティをめぐる進行中の論争といった、業界における重要な課題も詳しく紹介しています。

ヒューレット パッカード エンタープライズのHPEセキュリティ製品担当シニアバイスプレジデント兼ジェネラルマネージャーであるスー・バーサミアン（Sue　Barsamian）は次のように述べています。「2015年、攻撃者によるネットワーク侵入が憂慮すべきペースで発生し、過去最大級のデータ侵害につながりましたが、今はアクセルペダルから足を離して会社を厳重な隔離状態に置くべき時ではありません。私たちはこれらのケースから学び、リスク環境を理解、監視して、セキュリティを組織構造に組み入れて既知および未知の脅威をより効果的に軽減しなければなりません。これにより企業は大胆に革新を進め、ビジネスの成長を加速することが可能になります。」

〈アプリケーションが新たな戦場に〉
Webアプリケーションが企業に大きなリスクを発生させているのに対し、モバイルアプリケーションは増大する特徴的なリスクを生じさせています。
- モバイルアプリケーションは個人を特定可能な情報を頻繁に使用するため、個人情報や機密情報の保存および伝送において大きな脆弱性が生じます（*1）。
- スキャンの対象となったモバイルアプリケーションの約75%には、少なくとも1つの極めて重大もしくは深刻度の高いセキュリティ脆弱性が見つかりました。この割合はモバイル以外のアプリケーションでは35%でした（*1）。
- APIの悪用による脆弱性の件数では、モバイルアプリケーションがWebアプリケーションを大幅に上回るのに対し、エラー処理（エラーの予想、検出、解決）はWebアプリケーションの方が高い頻度で見られます（*1）。

〈パッチか消滅か〉
ソフトウェアの脆弱性悪用が依然として主たる攻撃ベクトルの一つであり、モバイルでの悪用が勢いを増しています。
- 前年と同様、2015年に悪用された脆弱性のトップ10は、発生後1年未満のものでした。68%は3年以上経過したものでした（*3）。
- 2015年、最も標的にされたソフトウェアプラットフォームはMicrosoft Windowsでした。発見された悪用のトップ20のうち、42%はMicrosoftのプラットフォームやアプリケーションを狙ったものでした（*3）。
- 2015年の悪用成功全体の29%は、これまでに2回パッチがあてられた、2010年のStuxnetの感染ベクトルを使用し続けていました（*3）。

〈マルウェアのマネタイゼーション〉
以前は業務に支障をきたすだけだったマルウェアは今や、攻撃者にとって収益を生み出す活動に変化しました。新たに発見されたマルウェアのサンプル総数は前年比で3.6%減少したものの、攻撃対象は変化する企業動向に合わせて著しく変化し、マネタイゼーションに大きな重点が置かれるようになりました。
- インターネットに接続されたモバイルデバイスの台数が増えるにつれ、マルウェアは最も人気の高いモバイルオペレーティングプラットフォームを標的にする形で多様化しています。Android系の脅威、マルウェア、および潜在的に迷惑なアプリケーションの数が増加し、毎日1万件以上の新たな脅威が発見されるようになり、全体の増加率は前年比153%に達しました。Apple iOSは伸び率が最も高く、マルウェアのサンプル数は230%以上の増加となりました（*2）。
- ATMへのマルウェア攻撃は、ハードウェア、またはATMに組み込まれたソフトウェア、あるいは両方の組み合わせを使って、クレジットカード情報を盗み出します。なかには、ソフトウェアレベルの攻撃によってカード認証を回避し、直接キャッシュを引き

出すケースも見られます（*2）。
・ Zbot Trojanの変種などのバンキング型トロイの木馬は、防御努力にもかかわらず問題であり続けており、2015年の検出件数は10万件を上回りました（*2）。
・ ランサムウェアは攻撃モデルとして、ますます成功を収めています。2015年には数種類のランサムウェアが、個人ユーザーや企業ユーザーのファイルを暗号化して大きな被害を及ぼしました。たとえば、Cryptolocker、Cryptowall、CoinVault、BitCryptor、TorrentLocker、TeslaCryptなどです（*2）。

〈対応策と推奨事項〉
・アプリが新たな戦場：ネットワーク境界の消滅とともに、攻撃者は焦点を移し、アプリケーションを直接狙うようになりました。セキュリティ専門家はこれに合わせてアプローチを調整しなければならず、ネットワークエッジだけでなく、場所やデバイスを問わず、ユーザー間のやりとりやアプリケーション、データも防衛しなければなりません。
・パッチか消滅か：2015年はセキュリティ脆弱性の報告件数とパッチの発行件数で過去最高を記録する年となりましたが、パッチは、もし予想外の影響を恐れてエンドユーザーがインストールしなければほとんど無意味です（*4）。セキュリティチームは企業ユーザーと個人ユーザーの両レベルでパッチの適用についてもっと警戒しなければなりません。ソフトウェアベンダーの側にも、エンドユーザーが恐れてパッチの導入をためらわないよう、パッチが及ぼしうる影響について情報の透明性が求められます。
・マルウェアのマネタイゼーション：企業や個人を標的にしたランサムウェア攻撃が増加しています。機密データや個人データが失われないよう、セキュリティ専門家の側に意識向上と備えの強化が求められています。ランサムウェアに対する最良の防御は、システム上のすべての重要ファイルを対象とする効果的なバックアップポリシーです。
・政治の変化に備える：複数の国にまたがる越境協定が、システムを安全で、法令遵守の状態に保とうと苦戦する企業に難題を突きつけます。組織は変化する立法活動を注意深くフォローし、柔軟なセキュリティ対応を維持しなければなりません。

〈調査手法〉
このサイバーリスクレポートは、HPEセキュリティリサーチが毎年発行するもので、セキュリティに関する喫緊の課題に関して詳細な業界データと分析を提供し、ビジネスリーダーとセキュリティ専門家の皆様に、ご自身のデジタルエンタープライズをより効果的に保護し、大胆にイノベーションを推進するための、対応策をご提案します。

調査方法に関する詳細はフルテキスト版のレポートを参照ください。
http://hpe.com/software/cyberrisk (英語版)

〈HPE Securityについて〉
HPE Securityは、企業がセキュリティを組織構造に組み入れ、高度な脅威を検出して対応し、継続性とコンプライアンスを保全してリスクを効果的に軽減することで、事業の根幹に関わるデジタル資産の保護をサポートします。市場をリードする製品、サービス、脅威対策、セキュリティ調査からなる総合的なパッケージを活用して、HPE Securityは企業が保護とイノベーションのバランスをとりながら今日のアイデアエコノミーに対応し続けることができるよう応援します。HPEセキュリティについての詳細は、https://www.hpe.com/us/en/solutions/protect-digital.html をご覧ください。

*1：HPE Security Research により2016年2月に発行された「2016年版サイバーリスクレポート」のHPE Security Fortify on Demand Findings ソフトウェア分析分野、p54-p63。
*2：HPE Security Research により2016年2月に発行された「2016年版サイバーリスクレポート」のマルウェア分野、p34-p51。
*3：HPE Security Research により2016年2月に発行された「2016年版サイバーリスクレポート」のエクスプロイト分野、p30-p33。
*4：2015年6月に発行されたHPE Security BriefingのEpisode 22。

■ プレスルーム
https://www.hpe.com/jp/ja/newsroom.html

# # #

■ お客様からのお問い合わせ先
カスタマー・インフォメーションセンター
TEL：0120-268-186 （携帯、PHS：03-5749-8279）
ホームページ：http://www.hpe.com/jp/