プレスリリース: 2016年07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、ハッキングビジネスの内部構造を解明

- 最新の「Business of Hacking」レポート（日本語版）により、サイバー犯罪の原動力となる敵対者のバリューチェーンを検証、企業の防衛強化に向けた実行可能な方策を提案 -

2016年7月22日

日本ヒューレット・パッカード株式会社

日本ヒューレット・パッカード株式会社（本社：東京都江東区、代表取締役社長執行役員：吉田 仁志、以下 日本ヒューレット・パッカード）は本日、サイバー犯罪を後押しする地下経済を広く検証した「The Business of Hacking（ハッキングビジネス）」レポートの日本語版を発行しました。今回の調査では、敵対者が実施しようとする攻撃の裏側にある動機と、犯罪組織がその領域を拡大し、収益を最大化するために確立した「バリューチェーン」を詳細に分析しています。本レポートでは、洞察に基づき、こうした敵対者グループを妨害しリスクを軽減するための、企業への実用的な推奨案も提供しています。

典型的なサイバー攻撃者の属性と、地下経済の相互接続的な性質は、過去数年間で著しく発展しています。今日の攻撃グループの大半にとって核となる動機は、自らの影響力と金銭的利益の向上です。敵対者は現在、最終的にはこの2つの動機を達成するため、オペレーションの作成と拡張において以前に増して高度な管理原則を活用しています。企業はこのような攻撃者の内部事情を活用することで、彼らの組織構造を妨害し、自社のリスクを軽減できます。

ヒューレット パッカード エンタープライズ(HPE)のHPE Securityサービス部門HPE Security Reserch責任者 兼 最高技術責任者であるアンジェイ・カワレック（Andrzej Kawalec）は、次のように述べています。「サイバーセキュリティを単にチェックするだけのチェックボックスのひとつと考えている企業は、高品質のサイバーセキュリティインテリジェンスの価値を活用していないのが一般的です。本レポートには、犯罪のバリューチェーンの各段階について、敵対者のオペレーションの方法や私たちが彼らを妨害できる方法などが、独自の視点で紹介されています。」

〈攻撃者の「バリューチェーン」〉
今日の敵対者は、様式化されたオペレーションモデルと、正規の事業構造と極めて類似した「バリューチェーン」を作成し、攻撃のライフサイクル全体を通じ、サイバー犯罪組織にとっての投資対効果（ROI）を高めることが一般的です。エンタープライズレベルのセキュリティリーダー、規制当局、法執行機関が、攻撃者の組織を妨害しようとする場合、こうした地下経済のバリューチェーンのあらゆる工程を理解することが先決です。

攻撃者のバリューチェーンモデルは、一般的には以下の重要な要素で構成されます。
・人材管理： 特定の攻撃要件を満たす上で必要なサポート「スタッフ」の獲得、審査、支払い。攻撃者のスキルベースのトレーニングや教育も、このカテゴリーに入ります。
・オペレーション： 攻撃のライフサイクル全体を通じた情報や資金のスムーズな流れを保証する「経営チーム」。このグループは、すべての工程でコストの削減とROIの最大化を積極的に模索します。
・技術開発： 研究、脆弱性の悪用、自動化など、所定の攻撃の実行に必要な技術的専門知識を提供する、前線の「労働者」
・マーケティングと営業： 同部門は、地下市場での攻撃グループの確固たる評価と、潜在的な購入者のターゲット層による違法商品の知名度と信頼を確立します。
・アウトバウンド物流： これには、大量の盗まれたクレジットカード情報、医療記録、知的財産など、購入者への商品の納品を担当する人とシステムの両方が含まれます。

IDCのセキュリティ製品およびサービス部門プログラム担当バイスプレジデントであるクリス・クリスチャンセン（Chris Christiansen）氏は、次のように述べています。「サイバー犯罪は高度に専門化しており、強力な資金源を有し、集中攻撃を仕掛けるために連携しています。HPEの『Business of Hacking』レポートは、敵対者のオペレーションと収益最大化の仕組みを理解することで、合法な組織が敵対者をより効果的に妨害し、リスクを軽減するための重要な洞察を提供します。」

〈バリューチェーンを妨害し、先進のエンタープライズ保護を提供〉
HPEでは、こうした組織的な攻撃者からより効果的な防御を実現するため、エンタープライズセキュリティの専門家に対し、以下をはじめ、さまざまなアプローチを推奨しています。
・収益の削減：「HPE SecureData」など、包括的な暗号化ソリューションを実装することで、企業への攻撃から敵対者が得られるであろう金銭的利益を制限します。保存データ、実行データ、使用データを暗号化し、情報を攻撃者にとって無用な形式とすることで、彼らの営業能力を制限して、収益を抑えます。
・ターゲットプールの削減： モバイルやIoTの普及により、すべての企業にとっては、潜在的な攻撃エリアが大幅に拡大しています。企業はセキュリティを自社の開発プロセスに組み込んで、デバイスの種類を問わず、データ、アプリ、ユーザー間のやり取りの保護に力を注ぐことで、敵対者の攻撃をより効果的に軽減おおよび妨害する必要があります。
・敵対者から学習： 「偽装グリッド」などの新技術は、本物そっくりに複製したネットワーク内を攻撃者に進ませることで、彼らを陥れ、監視し、学習する方法を実現しています。企業はこうした情報を活用することで、本物のネットワークをより効果的に保護し、同種の攻撃を開始前に妨害し、攻撃者の進行を遅らせることが可能です。

〈調査手法〉
「Business of Hacking」は、HPE Securityチームが収集したデータと観察、オープンソースのインテリジェンス、およびその他の業界レポートを活用することで、攻撃者の動機、組織、機会について、重要な洞察を生み出しています。これによって企業は、こうしたアクティビティをより効果的に妨害し、リスクを軽減できます。

本レポートの日本語版ダウンロードはこちらから(7月28日から)

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 Security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。

■ 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/