PwC's Cyber Intelligence

キャッシュレス社会
システム会社のエンジニアが狙われている

加速するキャッシュレス決済の普及

現在、世界的にキャッシュレス決済が推進され、既に私たちの日常生活にも浸透しました。

経済産業省の『キャッシュレス・ビジョン』(※1)によると、各国のキャッシュレス政策はさまざまな事情から実施されており、結果として経済状況を大きく好転させていることが分かります。

キャッシュレス決済は主にカード決済(クレジット、デビット、プリペイド)／電子マネー決済(ICカード、スマートフォン)／QRコード決済(スマートフォン)に分類され、特に後者2つは急速に市場を拡大しています。

キャッシュレス化の進展によって、支払いデータの利活用による消費の活性化や、実店舗などの無人・省力化、不透明な現金の流通の抑止による税収向上などにつながることが期待されています※1。今後も日本は政府主導のトップダウンによる強いキャッシュレス推進により、飛躍的にキャッシュレス決済の普及が進むと考えられます。

共有・悪用され続ける流出情報、パスワードリスト攻撃の危険性

このような中、経済産業省・金融庁・個人情報保護委員会による「キャッシュレス決済機能を提供する事業者の皆様への注意喚起」にも記載があるように、パスワードリスト攻撃の危険性が指摘されています※2。パスワードリスト攻撃とは、サイバー攻撃により情報流出したIDとパスワードの組み合わせを用いて、他のウェブサイトや電子マネーアカウントなどへのログイン試行を繰り返すものです。

ここ数年、オンラインショップをはじめとする多数のウェブサービスからログインID／パスワードなどのアカウント情報が流出し続けています※3。攻撃者は無差別に脆弱なウェブサイトを探索し、手当たり次第に攻撃していると思われ、一見サイバー攻撃被害とは縁の薄そうな、地方の観光情報サイトや行政サイトなどの一般ウェブサービスからの流出情報も多く見受けられます。こうして流出する情報の中には、流出の公式アナウンスやユーザーへの通知がなく、そもそも運営企業が攻撃を受けた事実に気付いていないと思われるものも含まれます。流出に至る経緯はさまざまですが、一度流出した情報はダークウェブなどで共有・販売され、ネット上から消えることはありません。

しかし、運営企業がサービスを安全に設計すれば攻撃の緩和は可能と思われ、また利用者がパスワードの使い回しを行わなければ他サービスへの2次被害を緩和できるとも考えられます。

以下に利用者／事業会社(ウェブサービスなどの運営企業)／システム開発会社それぞれが置かれている状況を整理し、どのように対応していくべきか、示唆を述べます。

pwc

出典
※1 経済産業省商務・サービスグループ消費・流通政策課, キャッシュレス・ビジョン(2020年7月15日閲覧)
※2 個人情報保護委員会、金融庁、経済産業省, キャッシュレス決済機能を提供する事業者の皆様への注意喚起(2020年7月15日閲覧)
※3 ITmediaエンタープライズ, 「7億7300万件の流出情報、闇フォーラムで流通　平文パスワードも出回る」(2020年7月15日閲覧)
※4 総務省, リスト型攻撃対策集について(2020年7月15日閲覧)
※5 日経XTECH, 「オムニ7」アプリのソースコードが流出、7payに続き新たな問題発覚(2020年7月15日閲覧)

【利用者】2段階認証サービスの利用で安全なキャッシュレス利用を

私たちが日常的に利用している各種ウェブサービスや電子マネーアカウントなどは、常に悪意のある犯罪者による攻撃の脅威にさらされています。利用者は、インターネット上に登録された自分の情報が流出して公開されてしまうことを前提として、自分の身を守るための最低限の努力をする必要があります。

強力なパスワードを設定することは、効果的な手段の一つです。情報流出は、誰の身にも起こり得ることです。パスワードを複数のサービスで使い回さず、また簡単に推測可能な一般的な単語などを避け、長い文字列を選択することで漏えいのリスクを軽減する必要があります。

また、IDおよびパスワードのみでログイン認証を行うウェブサービスの利用は控えること、IDとパスワードは上述の通り、推測可能文字列を使わずに、二段階認証などの安全なログイン方法を活用することが望ましいと考えられます。

【事業会社】セキュアな認証機構の導入を

経済産業省や総務省によるパスワードリスト攻撃への注意喚起もあり※2・※4、中小企業にもパスワードリスト攻撃の存在と手法が徐々に認識され始めました。同攻撃の代表的な事例として、キャッシュレス決済サービスへの不正アクセスが挙げられます。これは、他社サービスから流出したID・パスワードを使用してログイン試行が繰り返されたことによる被害と判明しています。脆弱な認証システムにより、攻撃に対する防御力が弱体化しているところを狙われました。また、大手企業のウェブサービスにおいて、外部からのパスワードリスト攻撃により、数千件を超えるアカウントが不正にログインされるという事象が発生しました。どちらも二段階認証などのセキュアな認証システムを導入していれば、未然に防げた可能性のある事例です。IDとパスワードのみでログイン可能な認証は避け、二段階認証やワンタイムパスワード、CAPTCHA認証など、よりセキュアなシステムを構築・運用する必要があると考えられます。

【システム開発会社】バージョン管理システムの利用に細心の注意を

ITシステムの開発会社は、バージョン管理システムの利用に注意する必要があります。

2019年、あるオンラインショップのアプリケーションのソースコードがバージョン管理システム上で外部公開されているのが見つかり、話題となりました※5。

セキュアなオンラインバージョン管理システムを利用していたとしても、公開リポジトリにソースコードやパスワードなどの機密情報をプッシュしている例は多く見られます。バージョン管理システムは、情報漏えいに気付いた利用者が削除したつもりでも実際には削除されずに復旧可能な場合が多く、攻撃者は日常的にこれらの情報を探索しています。

外部公開される可能性のあるオンラインシステムを、機密データを含むバージョン管理システムとして利用することは避ける必要があります。

狙われるエンジニアをいかに守るか

同時にシステム開発会社は、自社のエンジニアの保護にも力を入れる必要があります。2019年10月以降、北朝鮮が関与していると言われる悪意のあるハッカー集団・Lazarus Groupによるサイバー攻撃が、仮想通貨事業者を中心に、複数の国で観測・報告されています。北朝鮮の外貨獲得活動の一環と言われるこの活動は、金融分野の技術者を標的として行われており、近年増加傾向にあるものです。

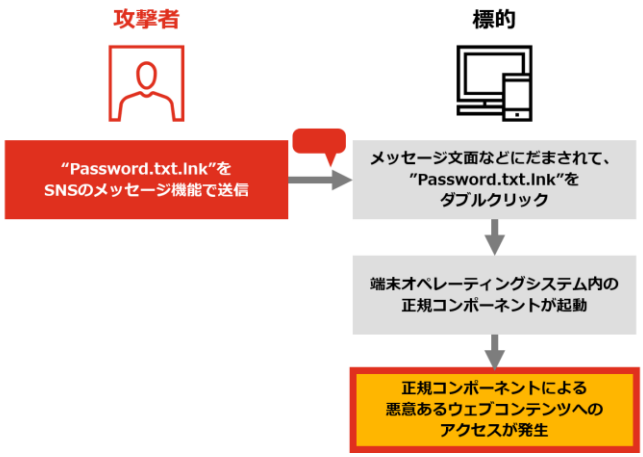
観測された攻撃キャンペーンでは、リクルーティング会社の社員を装った攻撃者が金融分野の開発者に対して、ビジネス特化型のSNSのメッセージ機能を通じてヘッドハンティングをかたって攻撃を行ったことが確認されています。同SNS上の当該アカウントが、同名のアカウントを乗っ取ったものなのか、実際の攻撃への協力者であるかは不明ですが、プロフィールに記載された所属組織への在籍は確認されていません。なお、同名のアカウントは、他の複数のSNSにも存在していました（図表1）。

図1：攻撃者のアカウント情報のイメージ

こうしたビジネス特化型SNSのメッセージ機能を利用した攻撃は、2019年1月に報告されたチリの金融サービス事業者へのサイバー攻撃でも使われており、Lazarus Groupが金融分野の技術者を標的とする際に好んで利用する手口です。

攻撃には、「Password.txt.lnk」というファイル名のショートカットファイルが悪用されています。標的に当該ショートカットファイルをクリックさせることで、オペレーティングシステム（OS）内に標準で存在する正規システムコンポーネントを起動させ、当該コンポーネントを介して、インターネット上の悪意あるウェブコンテンツへのアクセスを発生させるという手法です（図表2）。同様のショートカットファイルを悪用した攻撃は2019年にも、メールの添付ファイルを使用したものが観測されています。両者のサンプルを比較すると同一の構造であることが分かります。

図2：SNSのメッセージ機能を利用した攻撃の流れ



このようにLazarus Groupの攻撃の標的は、明らかにシステム開発者および運用者へと向き始めています。SNSとメールの併用が主な攻撃手法であると考えられており、開発会社は従業員に対して、SNS上で開示できる情報とできない情報をセキュリティ方針として定義し、SNS経由の情報流出やこうした攻撃に注意していく必要があります。

今回のポイント

1

キャッシュレス社会の到来と並行して、パスワードリスト攻撃の脅威が増加している。

2

現状、各種ウェブサービスなどからは恒常的に情報が流出し続け、それがダークウェブ上で拡散している。これを止める手段は事実上存在しない。

3

システム開発会社は従業員に対して、SNS上で開示できる情報とできない情報をセキュリティ方針として定義し、SNS経由の情報流出やサイバー攻撃に注意していく必要がある。

執筆者

名和　利男

PwC Japan グループ
サイバーセキュリティ
最高技術顧問

林　和洋

PwCコンサルティング
合同会社
パートナー

岩井　博樹

PwC Japan グループ
スレットインテリジェンス
アドバイザー

村上　純一

PwCコンサルティング
合同会社
ディレクター

PwC Cyber Security & Privacy

https://www.pwc.com/jp/ja/services/digital-trust.html