オンラインバンキングのセキュリティ

頻発するオンラインバンキング不正アクセス被害額は過去最高額と謳われている。犯行に利用されるツールのもつ機能を具体的に踏まえ、今できる防御について再考する。

相次ぐオンラインバンキング不正アクセス被害

2011年春ごろから、オンラインバンキングを悪用した不正送金が活発化した。悪用されたのはコンピュータ・ウィルスが詐取した正規の認証情報であり、システムの正常な処理を通して不正送金が行われている。その被害は今年4月から全国53の金融機関において、100件以上発生し、被害額は2億7000万円を超え過去最高との報告もある。一連の不正アクセス多発を受け、各機関はまず個人ユーザに向けた注意喚起を行ったが、その前に、犯行に利用されたコンピュータ・ウィルス自体が正確に理解されていただろうか。「敵を知り、己を知れば百戦危うからず」という諺を踏まえ、まずは「敵」の駆使する技術を紹介しつつ、次いで対策を考察する。

全知全能を謳うクライムウェア

情報漏洩の原因として名前が上がったのが、情報詐取に特化したZeus/SpyEyeと呼ばれるコンピュータ・ウィルスの類である。これらはクライムウェアと呼ばれる、犯罪目的での情報詐取に秀でた機能を持つプログラム群である。Zeus/SpyEye自体はすべてのWebアプリケーションで利用される情報を搾取できる機能を持っているが、

- 初期設定ファイルに著名な金融機関のオンラインバンキングシステムを狙う設定が既に記述されている
- 主に金融情報を狙うために利用されることが多い

という点が「バンキング系ウィルス」などに類する表現で呼ばれる所以であると思われる。

また、これらはPCだけでなく、スマートフォン用にも開発されつつあり、実際に情報詐取を行い、外部と通信するアプリケーションがいくつか発見されている。

コンピュータ・ウィルスというと、その動作内容は個体によって固定と考えがちであるが、Zeus/SpyEyeにおいては、動作部分と設定ファイルが分離しており、さらに、その挙動を任意タイミングで遠隔から制御可能であるために、「どのシステムを狙ったコンピュータ・ウィルスか？」などの観点で比較すると千差万別に近い。この仕様によって、個々の攻撃者の目的に沿った利便性を達成している。

攻撃者の設定次第で、この世にひとつだけのコンピュータ・ウィルスの完成となる。それがわずかな設定と数回のクリックで実現してしまう。作成されたコンピュータ・ウィルスは通信先や動作する状況が異なっており、特徴をつかみにくい。更に高度な隠ぺい技術を駆使して一定期間アンチウィルス製品による検知をかいくぐり、ユーザの端末に潜伏し、標的システムの情報を詐取する。

狙われたシステムに関する情報、奪った情報などは、暗号化された状態で送受信され、世界各地に用意した使い捨てのサーバを一時的に利用するなどの手法で犯行の痕跡ごと隠ぺいを図っている。

端末に潜伏するクライムウェアの機能

現在の主流バージョンにおいてコンピュータ・ウィルスの情報詐取機能に注目すると以下のようになる。

A.ブラウザとシステムで送受信する情報の詐取

標的システムに関するブラウザでのユーザの入力

NOTE

1) PCやスマートフォン、携帯電話上でワンタイムパスワードを生成する仕組み。文中では主に、PC上で生成する仕組みを想定して記述している。
2) 一度しか使えない使い捨てのパスワード。
3) ワンタイムパスワードを生成させるハードウェア。カード型やキーフォブ型が主に流通している。

と、システムがユーザを識別するための情報がすべて詐取される。また、端末に表示される画面の一部を改竄して、取引暗証番号やセキュリティコードなどの追加の入力を誘発して詐取しようとする機能もある。

また、電子証明書などの端末そのものを認証に利用するためのファイルも詐取可能であるため、端末認証が無効化される可能性がある。

B.ユーザ端末の画面の盗撮

攻撃者は任意時点でユーザ端末の画面を参照できる。したがって、ソフトウェアトークン[1)]により端末画面に表示されるワンタイムパスワード[2)]では、ユーザより先に攻撃者によって有効なパスワードを利用されたり、パターンの少ない乱数表を利用した認証では、複数回の盗撮にA.の機能を組み合わせると乱数表そのものを把握されたりする可能性がある。

C.ユーザ端末そのものを遠隔操作

Zeus/SpyEyeは遠隔からのデスクトップ接続を提供する。攻撃者は感染した端末を踏み台として経由し、標的システムにアクセスできる。端末ごとに固定な値を認識して認証に利用する仕組みや、電子証明書を利用した端末認証も突破される。

オンラインバンキングシステムの防御

前述したようにZeus/SpyEyeはユーザないし端末固定の情報を利用した認証方式そのものを脅かしている。ユーザの環境をクリーンな状態で完全に守ることができない以上、システムがユーザに入力を要求するすべての情報は「ある時点で」漏洩してしまうという前提を置き、システムの防御について再考しなくてはならなくなる。

ここまでは機能面のみ説明したが、実際の悪用を想起してみると、Zeus/SpyEyeは、システムとユーザの通信セッションに直接介入できず、情報を詐取するのみであり、攻撃者が詐取した情報を手動で入力して初めて不正アクセスが発生する。情報が詐取されるタイミングと、詐取された情報が使われるタイミングには少なからずタイムラグがある。そこで例えばハードウェアトークン[3)]が発行したワンタイムパスワードによる認証を情報表示、入出金、購入などの各重要処理において要求し、攻撃者が値を入手した頃には詐取した値が利用できなくなっていればよい。

この観点はログイン成功後のユーザ識別処理にも合わせて適用できるとより望ましい。ログイン毎に固定の値を利用したユーザ識別を行うのではなく、画面遷移毎など、より短い間隔で変化する値がユーザ識別に利用されていれば、その値が攻撃者に詐取され、利用される頃には無意味な値となっていることが期待できる。

最後に、対策実現にはコストや運用など大きな障害の付きまとうことが容易に推測されるが、「敵」が具体的に見えたことで、間違った情報や効果の薄い対策に惑わされなくなることにつながれば幸いである。まずは高額預金の条件にハードウェアトークンの利用を規約として入れるなど、利用用途を踏まえて柔軟に思考すれば、システム側で今できる防御も見えてくるのではないだろうか。

Writer's Profile

木内 雄章 Takenori Kiuchi
NRIセキュアテクノロジーズ
テクニカルコンサルタント
専門はセキュリティ診断
focus@nri.co.jp