お客様各位

2017年11月29日
グローバルセキュリティエキスパート株式会社

弊社の利用するメールアカウントの一つが不正メール送信に利用された

事象についてのお知らせ【第二報】

10 月 31 日に発生いたしました不正メール送信につきまして、調査が完了しましたので、対策および再発防止策をあわせて下記の通りご報告いたします。

記

1. 事象

2017 年 10 月 31 日（火）午前 5 時 7 分頃より、弊社のメール訓練サービスで使用しているメールサーバにある 1 つのメールアカウントが、外部からの不正アクセスを受けました。以後同日午前 10 時 15 分頃にアカウントを停止するまで、約 1 万 1 千件以上に上る、第三者に向けてのメール送信が行われました。

事象の発見と、収束に至る経緯は次の通りです。日付はいずれも 2017 年 10 月 31 日となります。

時刻	事象
午前 5 時 7 分	メールサーバ内に外部へ送信できないメールが滞留していることを示す通知が発生。
午前 9 時 15 分	以後、大量メール送信が開始されるまでの間に数回にわたりメール送信が発生。
午前 10 時 15 分	メールサーバから大量のメール送信が開始。

送信されたメール内容は次の通りです。

差出人	"From Western Union ..."<admin@safesitesweb.com>
件名	From Western Union / Money Gram ...
本文	Dear Beneficiary, After proper and several investigations and research at Western Union and Money Gram Office, we found your name in Western Union database among those that have sent money through Western Union and this proves that you have truly been swindled by those unscrupulous persons by sending money to them through Western Union/Money Gram in the course of getting one fund or the other that is not real. In this regard a meeting was held between the Board of Directors of WESTERN UNION, MONEYGRAM, the FBI alongside with the Ministry of Finance, As a consequence of our investigations it was agreed that the sum of Two Hundred And Fifty Thousand United States Dollars

	(U.S.250,000.00) should be AWARDED to you out from the funds that The United States Department of the Treasury has set aside as compensation payment for scam victims. This case would be handled and supervised by the FBI. We have submitted your details to them so that your funds can be delivered to you. Contact the Western Union agent office through the information below: Contact Person: Charles Williams .. Address: Western Union Post Office, Email: charleswilliams.office05@writeme.com Yours sincerely, James Robinson.

本文内容を要約すると「不正送金のお詫びに U.S.250,000.00 支払うので連絡をください。」という内容であり、受信者に対し、本文内の連絡先への連絡を誘導する、詐欺メールだと考えられます。
URL リンクの記載や添付ファイルはありませんでした。

送信先のドメインと送信件数の内訳は次の通りです。

ドメイン	件数
gmail.com	約 7,800 件
hotmail.com	約 1,500 件
その他（約 600 種）	約 3,000 件

過半数以上が gmail.com であり、ほとんどが海外のドメイン（yahoo.co.jp が 1 件のみ）です。
弊社の顧客ならびにメール訓練サービス対象のアドレスへの送信はありませんでした。

また同日内に、本事象以外にメールアカウントへの不正アクセス、メール訓練サービスで利用しているサーバへの攻撃の有無を確認しましたが、いずれも発見されませんでした。
本事象によるサービスへの影響は上記のみであると判断し、以後、サービスは継続しております。

2. 原因

当該メールアカウントおよびそのパスワードが漏洩し、不正アクセスに使用されたためと考えられます。
どのように漏洩したのかは現在のところ、判明しておりません。
但し、パスワードは攻撃に十分耐えうる、複雑なものを設定しておりました。またメールサーバ上のログには、パスワード総当たり攻撃に相当する数のログは記録されていないことから、過去および現在において弊社内に在籍し、かつ本パスワードを知り得た業務の従事者から、漏洩したものと推測しております。

3.　対策

本事象に使用されたメールアカウントの利用を停止すると共に、当サービスに関わるすべてのメールアカウントについて、利用の有無を確認しました。その上で、利用のないものは停止し、利用中のものは改めて個別に過去に使用されていないパスワードへ変更しました。
また以後、同様の事象が発生していないか、監視を継続しております。

4.　再発防止策

今回の事象発生の根本原因は以下 2 点と考えております。
1.　当該メールアカウントに、メール訓練以外の業務でも用いられていたパスワードを使用し、かつ長期間変更していなかったこと。
2.　メールアカウントおよびパスワードが判明すれば、第三者がメール送信可能な環境であったこと。

1. につきましては弊社内におけるパスワード運用のルールを再度検討し、パスワードの使いまわしが発生しえない仕組みづくりを進めてまいります。
2. につきましてはメールサーバの設定を再度点検し、本事象が発生しえない設定を検討して実施します。

加えて、今回のような事象発生の兆候を検知し、監視する体制の強化と、事象発生時における顧客およびパートナ様への連絡判断基準の検討を含め、社内体制および管理手順の見直しを進めてまいります。
これらの再発防止策の実施時期および具体策につきましては、改めてご報告します。

以上

【本内容に関するお問い合わせ先】
グローバルセキュリティエキスパート株式会社　経営企画本部
TEL　：03-3578-9001（代）