ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●Dropbox、2012年に6868万ユーザのアカウント情報を流出させていた･･･パスワードの変更を呼びかけ

http://www.itmedia.co.jp/enterprise/articles/1609/01/news073.html
http://gigazine.net/news/20160901-60-million-dropbox-account-stole/

このニュースをザックリ言うと･･･

- 8月25日（現地時間）、オンラインストレージ・データ同期サービス「Dropbox」(※1)より、2012年半ば以降パスワードを更新していないユーザに対し、パスワードを変更するよう注意喚起が出されました。

(※1)広く普及しているクラウドストレージ(オンラインストレージ)の一つで、インターネット上にファイルを保存できるストレージサービスの代名詞となっている

- 発表では、2012年6月にLinkedIn(※2) が不正アクセスを受けて奪取された1億1700万のアカウント情報が今年5月になってネットにアップロードされたことを受けての処置としていました。

(※2) 世界最大級のビジネス特化型ソーシャル・ネットワーキング・サービス

- その後8月30日、複数のネットメディアにより、同時期にDropboxからも不正アクセスにより6868万のアカウント情報が流出していたことが報じられ、Dropboxの社員にLinkedInの流出したアカウント情報と同じパスワードを使い回していた者がおり、そこから侵入されたとみられています。

- なお、流出したDropboxのパスワードはハッシュ化されており、現時点で悪用された形跡はないとされています。

AUS便りからの所感等

- Dropboxからは、2012年の時点で社員のアカウントが奪取され、同サービスへの不正アクセスに悪用されたことが発表されていましたが、アカウントの使い回しによる芋づる式の不正アクセスの脅威が警告される2014年頃よりも前の話であったことから、今年5月のLinkedInの件まで見落とされていた可能性が考えられます。

- ともあれ、連鎖的なアカウント情報の流出が数千万単位で発生するようになったことは決して見過ごせないものであり、各サービスにおいて異なるパスワード、かつ攻撃者が推測しにくいパスワードを設定するよう、改めて意識すべきでしょう。

- もちろん、マルウェアの感染によるパスワードの奪取の可能性についても忘れることなく、アンチウイルスやUTMによる防御を固めることもまた重要です。

ITmedia エンタープライズ

2016年09月01日 07時06分 更新

Dropboxのアカウント情報流出、被害は6800万件超に

2012年に起きたDropboxの情報流出事案で、盗まれたアカウント情報は6800万件を超えていたことが分かった。

[鈴木聖子，ITmedia]

米Dropboxが2012年に起きた情報流出事案に関連して一部ユーザーにパスワードの変更を促していた問題で、ニュースサイトのMotherboardは8月30日、盗まれたDropboxユーザーのアカウント情報は6800万件を超えていたことが分かったと伝えた。

Motherboardサイト

Motherboardによると、Dropboxユーザーのメールアドレスとハッシュ化されたパスワードを記録したファイルをデータベース取引関係筋から入手して調べたところ、ファイル4本に計6868万741件のアカウント情報が含まれていることが分かった。Dropboxの幹部もこれが同社のユーザーのものであることを確認したという。

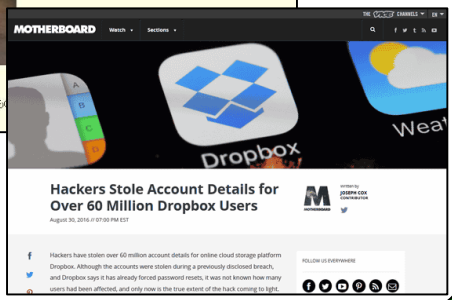
GIGAZINE

2016年09月01日 10時44分00秒

Dropboxが6800万件超のアカウント情報を流出させていたことが明らかに

By Ian Lamont

クラウドストレージサービスのDropboxが、なんと6800万件分も
た。



●ランサムウェア感染、身代金でデータを取り返せたのは45%

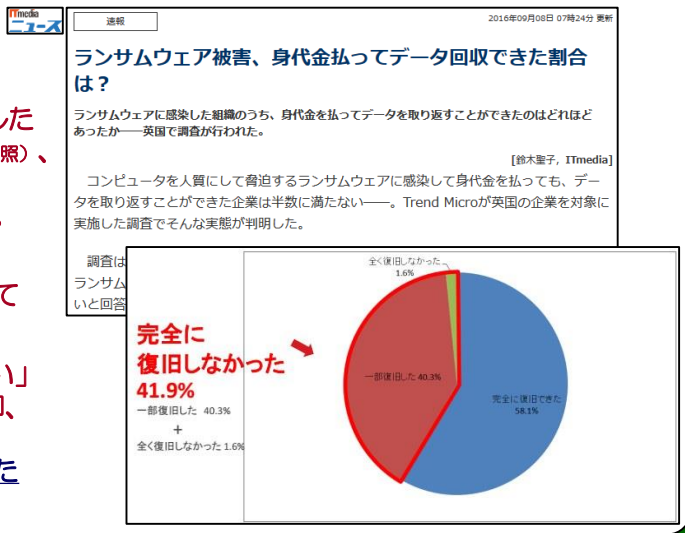
http://www.itmedia.co.jp/news/articles/1609/08/news083.html

このニュースをザックリ言うと・・・

- 9月7日（現地時間）、大手セキュリティベンダーのトレンドマイクロ社より、8月に英国企業（従業員1000人以上）のIT担当者を対象に行ったランサムウェア被害に関する調査結果が発表されました。

- 調査によれば、ランサムウェアに感染したことのない組織の74%は「感染したとしても身代金は払わない」と回答したとのことですが、一方、実際に感染した組織の65%が「身代金を払った」と回答しており、そのうち実際にデータを取り返せたのは45%のみだったとされています。

- また、感染しても身代金を払わなかった企業について、そのうち60%がバックアップからデータを復旧できたと回答しています。


速報

2016年09月08日 07時24分 更新

ランサムウェア被害、身代金払ってデータ回収できた割合は？

ランサムウェアに感染した組織のうち、身代金を払ってデータを取り返すことができたのはどれほどあったか――英国で調査が行われた。

[鈴木聖子，ITmedia]

コンピュータを人質にして脅迫するランサムウェアに感染して身代金を払っても、データを取り返すことができた企業は半数に満たない――。Trend Microが英国の企業を対象に実施した調査でそんな実態が判明した。

調査は
ランサム
いと回答

完全に復旧しなかった 41.9%
一部復旧した 40.3%
＋
全く復旧しなかった 1.6%

全く復旧しなかった 1.6%
一部復旧した 40.3%
完全に復旧できた 58.1%

AUS便りからの所感等

- トレンドマイクロ社からは8月にも国内企業を対象にした同様の調査結果が発表されており（AUS便り 2016/08/08号参照）、こちらもランサムウェアに感染した組織の62.6%が「身代金を払った」と回答した、等の結果が出ています。

- ランサムウェアの開発者は「身代金を払えばデータを返してくれるかも」という期待を絶妙なさじ加減で煽っているようにも見えます。

- ともあれ「感染したら基本的にはデータは取り返せない」と認識した上でのアンチウイルスやUTMによる感染防御、そして「感染は100%防げるわけではない」と意識し、データバックアップを確実にとることとバックアップしたデータも感染しないよう注意をはらうことが肝要です。

●中国最大級の認証局、SSL証明書の不適切な発行が可能だった

http://gigazine.net/news/20160901-wosign-fake-certificate/

このニュースをザックリ言うと・・・

- 8月30日（現地時間）、セントラルフロリダ大学医学部のサイト管理者により、SSL証明書を発行する認証局としては中国最大級の「沃通(WoSign)」が不適切なSSL証明書の発行が可能な状態であったことが発表されました。

- 発表によれば、管理者はWoSignの無料サービスを利用し、自分が管理する学部のサブドメインのためのSSL証明書を発行しようとしたところ、誤って自分が権限を持たない大学のドメイン(ベースドメイン)のための証明書発行をリクエストしたにも拘らずその証明書が発行されたとしており、管理者はWoSignにこの問題を報告したものの、WoSignが不適切に発行した証明書の無効化を行っている様子はない模様です。

- Firefoxブラウザの開発者の間では、WoSignのルート証明書を無効化することが話し合われているとのことで、中国国内のSSL対応Webサイトの3つに1つはWoSignの証明書を使っているとされており、無効化された場合の影響は大きなものになるとみられます。

AUS便りからの所感等

- ドメインの本来の所有者以外に偽のSSL証明書が発行されるケースとしては、今回は、認証局への不正アクセスではなく、証明書発行プロセスに「脆弱性」が存在していたという点で独特のケースと言えます。

- 偽のSSL証明書を入手した攻撃者は、これを偽のサーバに導入し、いわゆる「DNSキャッシュ汚染」等と組み合わせて、ユーザを偽のサーバに誘導するといった攻撃を行うことができ、このとき、攻撃を受けたユーザは、SSL証明書から本物のサイトと正常な通信を行っていることを確認できず、攻撃者に暗号化された通信内容を傍受される恐れがあります。

- これまでの事例の多くは、認証局および各OS・ブラウザベンダー・セキュリティベンダーが密に連絡を取り合い、偽の証明書の失効、ブラックリストへの登録等を迅速に行ったことにより、被害は最小限に抑えられていましたが、今回についても、WoSignには安全を確保するための適切な対応を期待したいところです。