— AUS（アルテミス・ユーザ・サポート）便り 2016/11/21号 —
http://www.artemis-jp.com

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。

●新生銀行グループ企業で債務者名など計38件漏洩か、感染検知も駆除できず

http://itpro.nikkeibp.co.jp/atcl/news/16/110403263/
http://www.itmedia.co.jp/enterprise/articles/1611/08/news119.html

このニュースをザックリ言うと･･･

- 11月4日（日本時間）、新生銀行より、グループ会社の新生インベストメント＆ファイナンス(SIF)社のPC1台がマルウェアに感染し、情報漏洩が発生した可能性があると発表されました。

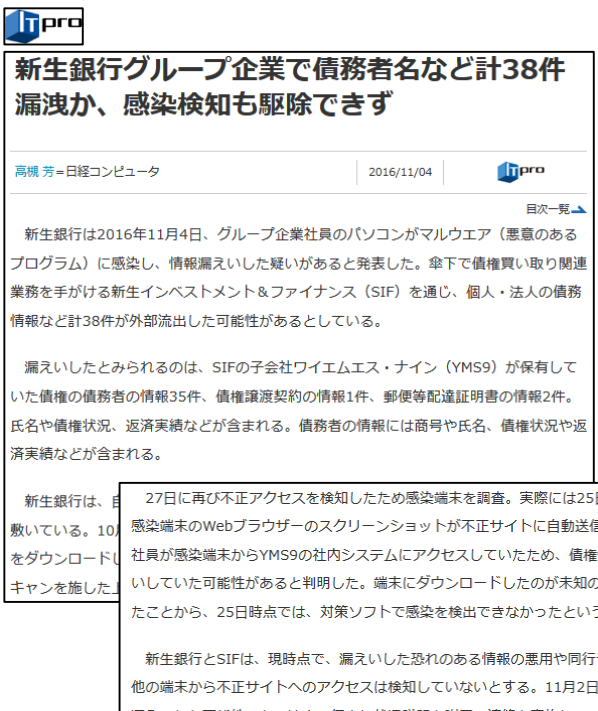
- 発表によれば、10月25日に当該PCがなりすましメールによるマルウェアをダウンロードしたことを新生銀行のセキュリティシステムが検知、一旦マルウェアチェックを行いましたが、同27日に当該PCから外部への不正な通信を検知、再度チェックした結果、25日の段階では検出されていなかったマルウェアが当該PCのスクリーンショットを外部に送信していたことが明らかになったとのことです。

- これにより、SIF社の子会社が保有する、債権の債務者の情報35件、債権譲渡契約情報1件、および郵便等配達証明書情報2件の計38件が漏洩したとみられています。

AUS便りからの所感等

- 日々数えきれないほどの新しいマルウェアや亜種が発生しており、アンチウイルスソフトやUTMによる対応において、パターンファイルにそれらのマルウェアの情報を登録していく形式をとる限り、タイムラグが発生することも残念ながら決して珍しい話ではありません。

- 一部アンチウイルスベンダーでは、パターンファイルに依存せず、マルウェアの不正な挙動にフォーカスした「振る舞い検知」と呼ばれる技術を用いており、未知のマルウェアにも対応可能とされていますが、この機能の実装には非常に高い技術力が要求されており、アンチウイルスやUTMで今後どれだけ実装され広まっていくかが注目されます。



新生銀行グループ企業で債務者名など計38件漏洩か、感染検知も駆除できず

高槻 芳＝日経コンピュータ　2016/11/04

目次一覧

新生銀行は2016年11月4日、グループ企業社員のパソコンがマルウエア（悪意のあるプログラム）に感染し、情報漏えいした疑いがあると発表した。傘下で債権買い取り関連業務を手がける新生インベストメント＆ファイナンス（SIF）を通じ、個人・法人の債務情報など計38件が外部流出した可能性があるとしている。

漏えいしたとみられるのは、SIFの子会社ワイエムエス・ナイン（YMS9）が保有していた債権の債務者の情報35件、債権譲渡契約の情報1件、郵便等配達証明書の情報2件。氏名や債権状況、返済実績などが含まれる。債務者の情報には商号や氏名、債権状況や返済実績などが含まれる。

新生銀行は、自
敷いている。10
をダウンロード
キャンを施した

27日に再び不正アクセスを検知したため感染端末を調査。実際には25日から27日まで感染端末のWebブラウザーのスクリーンショットが不正サイトに自動送信されていた。社員が感染端末からYMS9の社内システムにアクセスしていたため、債権情報などを漏えいしていた可能性があると判明した。端末にダウンロードしたのが未知のマルウエアだったことから、25日時点では、対策ソフトで感染を検出できなかったという。

新生銀行とSIFは、現時点で、漏えいした恐れのある情報の悪用や同行やグループ内の他の端末から不正サイトへのアクセスは検知していないとする。11月2日から順次、情報漏えいした可能性のある法人・個人に状況説明と謝罪の連絡を実施しているという。

2016年11月08日 17時53分 更新

新生銀行子会社で情報漏えいの可能性、「未知のマルウェア」と後から判明

セキュリティシステムでマルウェアのダウンロードが検知されたものの、ダウンロード先PCのセキュリティソフトでは検知できないものだったという。

[ITmedia]

印刷／PDF　71 ツイート　77 いいね！　77 シェア　9 Bookmark　12 Pocket　5 G+1　共有する　通知

新生銀行は、同社グループ会社の新生インベストメント＆ファイナンス（SIF）で、マルウェアに感染したPCから情報漏えいした可能性があることを明らかにした。監視システムでマルウェアのダウンロードを検知したものの、セキュリティソフトでは検知されなかったという。

新生銀行によると、同行ではSIFを含む一部のグループ会社にネットワークインフラを提供し、サイバーセキュリティの監視、運用管理も行っている。10月25日にセキュリティシステムがSIF社員のPCでのマルウェアのダウンロードを検知し、同日中にこのPCをネットワークから隔離して、セキュリティ対策ソフトによるスキャンを実施し、ネットワークに戻した。マルウェアは、社員が受信した「なりすましメール」から誘導された外部サイト経由で侵入したとみられる。

新生インベストメント＆ファイナンスのWebサイト

●佐川急便の不在通知を装ったスパムメール

http://www2.sagawa-exp.co.jp/whatsnew/detail/721/

このニュースをザックリ言うと・・・

- 11月15日（日本時間）、佐川急便より、同社からの発送や不在通知を装ったスパムメールについて注意喚起が出されています。

- 今回確認された例として、「佐川急便 商品発送のお知らせ」という件名でマルウェアとみられるファイルが添付されているもの、および「サガワ運送」という差出人、「宅配便お届けのお知らせ」という件名で、フィッシングサイトへのリンクが貼られているものが挙げられています。

AUS便りからの所感等

- フィッシング等のメールについては同社から度々注意喚起が出されており、前述したURLの情報は数年以上更新され続けています。

- 正式なサービスへのアクセス、あるいは不審なメールに関する相談など、同社サイトへのアクセスにあたっては、メールに記載されたURLのクリックは避けましょう。

- あらかじめブックマークに登録したURLからアクセスするようにし、ブラウザ・アンチウイルス・UTM等のアンチフィッシング機能を有効にすることは、当AUS便りでも度々推奨しております。

●不正なPDFファイルのアップロードによる攻撃の可能性

http://www.itmedia.co.jp/enterprise/articles/1611/14/news134.html

このニュースをザックリ言うと・・・

- 11月14日（日本時間）、IPAおよびJPCERT/CCより、PDFの仕様を悪用した、不正なPDF文書による攻撃の可能性が存在すると発表されました。

- 発表によれば、「Adobe社のPDFリーダー(Adobe ReaderおよびAcrobat Reader DC)に付属するプラグインがユーザのブラウザ(IEおよびFirefox)で有効になっている」かつ「攻撃者がPDFファイルをユーザが利用しているWebサーバにアップロード可能」な場合、サーバ上のPDFファイルをブラウザから開くことにより、情報漏洩や任意のスクリプト実行等の不正行為が行われる可能性があるとのことです。

- 発表では、回避策として、当該プラグインを無効にすることが推奨されています。

AUS便りからの所感等

- 発表によれば、PDFの規格（PDF 1.5以降）上の仕様（PDF文書に入力フォームを埋め込む「Adobe XML Forms Architecture(XFA)」およびスクリプトを埋め込む「FormCalc」）に含まれる、WebサーバとのHTTP通信を行う機能を悪用する攻撃とのことで、Adobe製PDFリーダーのブラウザ向けプラグインがこの機能に対応しています。

- PDFファイル上で指定された任意のスクリプトがブラウザ上から実行され、PDFファイルが置かれていたWebサーバに不正にアクセスされる等の可能性があることから、クロスサイトスクリプティング（XSS）やクロスサイトリクエストフォージェリ（CSRF）と同様の影響が発生するとされています。

- PDFファイルをブラウザ上で開く場合、現在のFirefoxではPDFリーダー機能を自前で搭載しています（ChromeやEdgeでも同様）ので、そちらを用いる方がまだ安全でしょうし、この他の回避策としては、PDFファイルを一旦ダウンロードしてから開くこと、その際にもなるべくAdobe製リーダー以外を使うこと等が挙げられます。