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。

●新種ウイルスによる不正送金摘発…被害2億円超

http://www.tokyo-np.co.jp/article/national/list/201710/CK2017100502000292.html
https://mainichi.jp/articles/20171005/k00/00e/040/229000c

このニュースをザックリ言うと・・・

- 10月5日（日本時間）、警視庁サイバー犯罪対策課より、インターネットバンキングを狙うマルウェア「DreamBot」の感染により不正送金された預金を5月に引き出した容疑で、埼玉県の男を逮捕したと発表されました。

- DreamBotは今年3月に国内で初めて確認され、オンラインバンキングサイトへのアクセス時にワンタイムパスワードを要求する偽のフォームを表示する等の特徴があります（AUS便り2017/3/27号参照）。

- 同庁では昨年11月から今年6月にかけ、24都府県で計93件、約2億4500万円にのぼる過去最大規模の不正送金被害を確認しており、いずれも今回逮捕された男らの同一グループによるもの、また大半がDreamBot絡みのものとみられています。

AUS便りからの所感等

- 警視庁が発表した今年上半期（1～6月）に全国で起きた不正送金被害額は5億6400万円で、うち半数近くが今回摘発されたグループによるものとなっています。

- 日本サイバー犯罪センター（JC3）は3月以降、特にDreamBotやその原型とされる「Gozi(URSNIF)」について注意を呼び掛け、PCがそれらに感染していないかチェックするサイト（https://www.jc3.or.jp/info/dgcheck.html）も用意しています（ただし感染の検出を完全に保証するものではないことに注意が必要です）。

- マルウェアに感染する可能性を抑止するためには、日頃からのアンチウイルスによるウイルスチェックやUTMによる防御等、各種防衛手段との組合せが肝心となり、また、ログインや送金処理の際、厳密な確認のためスマホアプリを用いるケースも増えてきていますので、スマホを狙う攻撃に対しても同様にアンチウイルスの導入やUTM経由での使用等の対応を行うべきです。

東京新聞 TOKYO Web

新型ウイルス、不正送金か　被害2億円超　窃盗容疑で男逮捕

ツイート B! 0 シェア 3 G+

2017年10月5日 夕刊

他人のインターネットバンキング口座から不正送金させた金を引き出したとして警視庁は五日、窃盗疑いで埼玉県川口市西川口二、無職武村維先(いせん)容疑者(31)を逮捕したと発表した。

逮捕容疑では五月八日、コンピューターウイルスに感染した東京都内の三十代男性のパソコンから不正送金された金融機関の口座から、約八万六千円を引き出したとされる。サイバー犯罪対策課によると、引き出した金で電子マネーのプリペイドカードを購入し、カード番号を犯行グループの上役に伝えていたという。「ボスから指示されて金を受け取っただけ」と容疑を否認している。

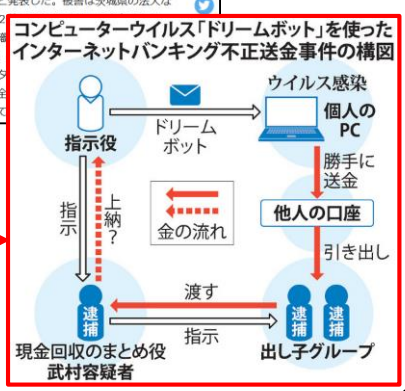
同課は昨年十一月～今年六月、全国二十四都府県で九十三件、計約二億四千五百万円の過去最大規模の不正送金被害を確認。被害の大半は「DreamBot(ドリームボット)」と呼ばれる新種のウイルスが使われていた。今年上半期の被害額は、全国の不正送金被害の半分近くを占めた。

いずれも同一グループにより引き出されており、警視庁は六月、金の引き出し役の中国人の男二人を逮捕。送金先は、外国人留学生らから不正に買い取った口座だった。武村容疑者もメンバーの一人で、同課は今回の犯行もドリームボットによるものとみている。

毎日新聞

警視庁

新種ウイルスで不正送金　被害２．４億円　摘発



●Office 2007、来週10月10日にサポート終了、40万台以上のPCで利用

http://itpro.nikkeibp.co.jp/atcl/news/17/100402401/

このニュースをザックリ言うと・・・

- 10月4日（日本時間）、大手セキュリティベンダーのトレンドマイクロ社より、同10日に延長サポートが終了する「Microsoft Office 2007」について、9月末における利用状況の調査結果が発表されました。

- Office全体での利用率こそ8.60%（12人に1人）まで減少しているとはいえ、依然40万台以上のPCで利用されているとの結果が出ています。

- 同社では、サポート終了後はセキュリティパッチが提供されず、脆弱性を突かれてPCの乗っ取りや情報漏洩が発生する可能性があるとし、最新バージョンであるOffice 2016等へのアップグレードを呼び掛けています。

AUS便りからの所感等

- 今年は4月にWindows Vistaもサポートが終了していますが、トレンドマイクロ社ではこちらも依然1.57%のPCが使い続けているとの結果を発表しています。

- Office 2010以降に採用された「保護されたビュー」により、不正なOfficeファイルによるマルウェアのダウンロード等を阻止できる可能性がありますが、2007にはこの機能がありませんので、より新しいバージョンへのアップグレードを推奨致します。

- そして古いバージョンを当分使い続ける必要がある場合は特に、アンチウイルスやUTM等により、マルウェアへの感染の可能性を少なからず低減させることが重要です。

●2013年に発生していた米Yahoo!でのアカウント流出、全ユーザ30億にのぼっていた可能性

http://internet.watch.impress.co.jp/docs/news/1084314.html

このニュースをザックリ言うと・・・

- 10月3日（現地時間）、米「Yahoo!」を現在運営するOath社より、2013年8月に発生していたユーザ個人情報流出事件についてのさらなる調査結果が発表されました。

- 2016年12月の発表（AUS便り 2016/12/26号参照）時点では、被害を受けたアカウント数は約10億人分とされていましたが、今回の発表で、当時のYahoo!全ユーザにわたる30億人分が流出の被害を受けた可能性があることが明らかになっています。

- 流出した情報は、ユーザの氏名・メールアドレス・電話番号・生年月日・ハッシュ化されたパスワードおよび秘密の質問と回答等とされており、ハッシュ化されていないパスワードや銀行口座情報等は含まれておらず、またYahoo! JAPANのユーザについては影響はないとのことです。

AUS便りからの所感等

- パスワードがハッシュ化されていたとはいえ、MD5という今となっては古いハッシュアルゴリズムが用いられており、元のパスワードが割り出される可能性は高いとみられます。

- 少なくとも2016年に流出が明らかになった時点でパスワードを変更していなかったユーザについては、今回は必ず変更すること、いわゆる「パスワードリスト攻撃」の標的にならないため他のサービスで使っていないパスワードであること、が重要です。

- こういったWebサービス等のアカウントで最も注意すべきなのは、利用しなくなって数年たっているユーザであり、放置していたアカウントに不正ログインされ、不正行為が行われることがないよう、自分が登録したサービスについて可能な限り全て把握しておくことが大事です。