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。

●「偽画面にご注意！」を偽画面に表示、三菱東京UFJ銀行をかたるフィッシング

http://itpro.nikkeibp.co.jp/atcl/news/15/012300286/
http://www.bk.mufg.jp/info/phishing/20131118.html?link_id=p_top_juyo_mail

このニュースをザックリ言うと･･･

- 1月23日（日本時間）、フィッシング詐欺に関する調査・啓発を行っているフィッシング対策協議会より、三菱東京UFJ銀行を騙る（かたる）フィッシングの報告を複数受けているとして警告が出されています。

- 警告において例に挙げられているフィッシングサイトのURLは「bk.mufg.jp」が含まれているものもあるものの、いずれもjpドメイン以外のcomドメインやcnドメインによるものです。

- 協議会では、①フィッシングサイトにてアカウント情報（ご契約番号、パスワード等）を絶対に入力しないこと、②万が一誤って入力した場合には銀行の緊急連絡先などに連絡すること、③類似のフィッシングサイトやメールを発見した際には同協議会へ連絡すること、などを呼びかけています。

AUS便りからの所感等

- フィッシングサイトは、その気になれば本物のサイトからコピーすることにより、本物と全く見分けがつかないレベルのログイン画面を用意することも可能です。

- 本物のサイトのログイン画面では大抵「EV-SSL」という特別なSSL証明書が使用されており、多くのブラウザでそれを利用していることを視覚的に確認できますし、また、メールに記載されているリンクを経由してログイン画面にアクセスするのではなく、ブラウザのブックマークに登録しておくこともフィッシングの回避策としては効果的でしょう。

- 一方で、「PCに感染したマルウェアにより、本物のサイトへのアクセス時に偽のログインフォームを表示する」という手法も多く使われていますので、そちらの方面についても、アンチウイルスやUTMの導入による防御を怠りなく実施することが肝要です。


ニュース　日経コンピュータ

「偽画面にご注意！」を偽画面に表示、三菱東京UFJ銀行をかたるフィッシング

2015/01/23
勝村 幸博＝日経コンピュータ（筆者執筆記事一覧）

記事一覧へ >>

125 おすすめ　13 共有　5 ブックマーク　17 Pocket　56 ツイート　シェア

フィッシング詐欺対策の業界団体であるフィッシング対策協議会は2015年1月23日、三菱東京UFJ銀行をかたるフィッシング詐欺が複数報告されているとして注意を呼びかけた。偽メールに記載されたURLにアクセスすると、「偽画面にご注意！」との表示がある、本物そっくりの偽サイトに誘導される（画面1）。

フィッシング詐欺とは、有名な企業や組織をかたった偽メールや偽サイトでユーザーをだまし、個人情報などを盗むネット詐欺のこと。典型的な手口は、偽サイトのURLを記載した偽メールを不特定多数に送信。実在するWebサイトのログインページなどに見せかけた偽サイトに誘導して、パスワードなどを入力させる。

画面1● 三菱東京UFJ銀行をかたるフィッシングサイトの例（フィッシング対策協議会の情報から引用）
[画像のクリックで拡大表示]

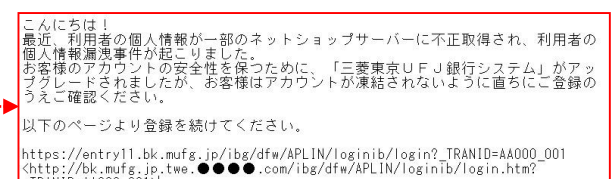
画面2● 三菱東京UFJ銀行をかたるフィッシングメールの例（フィッシング対策協議会の情報から引用）
[画像のクリックで拡大表示]


三菱東京UFJ銀行

偽画面にご注意！

ログイン

インターネットバンキングヘルプデスク 0120-543-555


こんにちは！
最近、利用者の個人情報が一部のネットショップサーバーに不正取得され、利用者の個人情報漏洩事件が起こりました。
お客様のアカウントの安全性を保つために、「三菱東京ＵＦＪ銀行システム」がアップグレードされましたが、お客様はアカウントが凍結されないように直ちにご登録のうえご確認ください。

以下のページより登録を続けてください。

https://entry11.bk.mufg.jp/ibg/dfw/APLIN/loginib/login?_TRANID=AA000_001
<http://bk.mufg.jp.twe.●●●●.com/ibg/dfw/APLIN/loginib/login.htm?_TRANID=AA000_001>

●朝日新聞社のPCがウイルス感染、1ヶ月以上情報が漏洩

http://itpro.nikkeibp.co.jp/atcl/news/15/011700198/
http://www.asahi.com/articles/ASH1J55L6H1JULZU00M.html

このニュースをザックリ言うと・・・

- 1月16日（日本時間）、朝日新聞社は、自社のPC17台がウイルスに感染し、情報の流出が発生していたことを発表しました。

- ウイルスへの感染による情報の流出は、昨年11月下旬頃から発生し、社内外とやり取りした電子メール等が流出したとされていますが、新聞読者および朝日新聞デジタルのユーザに関する情報の流出は確認されていないとのことです。

- 同社では1月9日に感染したPCが外部と通信を行っていることを確認し、対策を講じた上で警視庁に届け出たとのことです。

AUS便りからの所感等

- PCに感染したマルウェアの活動は必ずしも一目で分かりやすいものではなく、長期間気付かれずに外部と通信を行うケースや活動開始まで潜伏するケースも珍しくはありません。

- まずは、アンチウイルス等による随時PCの感染チェックが最低限必要な対策であり、さらにUTMの設置による外部との不審な通信の遮断が機密情報の流出を食い止めるのに効果を発揮することでしょう。

ニュース　日経コンピュータ

朝日新聞社でPC17台がウイルス感染、外部サーバー通じ1カ月以上情報が漏洩

2015/01/17
斉藤 栄太郎＝日経コンピュータ（筆者執筆記事一覧）

記事一覧へ >>

33　10　13　43　115
おすすめ　共有　ブックマーク　Pocket　ツイート
シェア

朝日新聞社は2015年1月16日、社内のPC17台がウイルスに感染し、社内外とやり取りした電子メールなどの情報が流出したと発表した。既に感染したPCからの新たな情報流出を防ぐ措置を講じたと共に、警視庁に届け出たとしている。

発表によると、同社がウイルス感染に気付いたのは1月9日の夜。社内のPCが外部のサーバーと不審な通信をしていることが発覚したという。外部サーバー（一般にC＆Cサーバーと呼ばれる。C＆Cは「コマンド・アンド・コントロール」の略）から指示を受けてPCから情報を盗み出すなどの活動を行う、いわゆる「バックドア型不正プログラム」に感染したとみられる。

情報の流出は2014年11月下旬ごろに始まったとしており、1カ月以上にわたって社外に情報が流出し続けていたことになる。流出が確認された情報の種類は電子メールやPCで作成した文書などの一部であるとしており、「新聞読者や朝日新聞デジタルの顧客に関する情報の流出は確認されていない」（朝日新聞社）としている。ただし、「引き続き確認を進める」とも付け加えている。

●「Winny」等P2Pファイル共有ソフトの利用者は依然15万人に

http://itpro.nikkeibp.co.jp/atcl/news/15/013000357/
http://www.netagent.co.jp/product/p2p/report/201501/01.html

このニュースをザックリ言うと・・・

- 1月30日（日本時間）、セキュリティベンダーのネットエージェント社がP2Pファイル共有ソフトの利用状況調査の最新結果を発表しました。

- P2Pファイル共有ソフトの中でも代表的とされる「Winny」「Share」「Perfect Dark」について、昨年12月27日から1月4日にかけての利用者数を調査した結果、現在でも延べ15～20万人がこれらを定期的に利用しているとされ、うちWinnyとPerfect Darkが4万5千人前後、Shareが3万人前後となっています。

- 一方、これらのソフトの利用による検挙･逮捕の割合では、「Share」が49%と最も多くなっています。

AUS便りからの所感等

- P2Pファイル共有ソフトが猛威を振るった2000年代には、企業のPC上にインストールして使用するようなケースは珍しくなく、ウイルスへの感染による企業の機密情報が流出するような事件も多発していました。

- 警察による監視と検挙、ISPによる通信の規制が一般的になった現在でも、規制が緩いISPの情報等がWeb上でやり取りされる等により、依然根強いユーザがいるのが現状のようです。

- 近年のUTMには、こういったP2Pによる通信を識別して遮断する機能にも対応していますので、情報流出を防ぐための出口対策として利用することが効果的です。

ニュース　日経コンピュータ

「Winny」などの利用者は15万人、逮捕者の半数は「Share」が原因

2015/01/30
勝村 幸博＝日経コンピュータ（筆者執筆記事一覧）

記事一覧へ >>

1　1　5　24　36
おすすめ　共有　ブックマーク　Pocket　ツイート
シェア

セキュリティベンダーのネットエージェントは2015年1月30日、年末年始（2014年12月27日から2015年1月4日）に同社が観測した、P2Pファイル共有ソフトの利用者数（ノード数）を発表した。現在でもおよそ15万人が定期的に利用しているという。

調査対象は、代表的なP2Pファイル共有ソフトの「Winny（ウィニー）」「Share（シェア）」「Perfect Dark（パーフェクトダーク）」。ネットエージェントでは独自のシステムでこれらのソフトの利用状況を継続的に観測している。今回発表したのは、2014年～2015年の年末年始における利用状況。