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。

●SEOポイズニングにPDFを用いた新手法…PDFファイルの差し替えを行い不正なサイトへ誘導

http://news.mynavi.jp/articles/2015/07/10/seo/
http://news.mynavi.jp/articles/2015/07/13/seo/

このニュースをザックリ言うと・・・

- Google等サーチエンジンの検索結果で上位に表示されるための「検索エンジン最適化(SEO)」を悪用し、悪意のあるサイト等を上位に表示させる「SEOポイゾニング」の手口について、セキュリティベンダーであるSophos社のブログにおいて解説されています。

- SEOポイゾニングの手法の一つに、サーチエンジンに対し通常と異なるページを提示する「クローキング」がありますが、記事では、同社のアンチウイルスが連日多数の疑わしいPDFファイルを検出したことから、Googleが行っているクローキング対策を回避するためにそういった手法を用いていることを発見したとのことです。

- 攻撃者は、合法的なWebサイトをクラックしてPDFファイルを差し替えているとみられ、これにより、検索結果の上位に表示されるPDFファイルに含まれるリンクから、マルウェアをダウンロードさせるような不正なサイトへ誘導する、という手法をとっている模様です。

AUS便りからの所感等

- 検索結果の上位にあるコンテンツを不正なものにすり替える手法は従来から攻撃者がよく狙うものであり、中には攻撃者自身が一見安全に見えるサイトを立ち上げ、上位に表示されるようになった頃合で不正なコンテンツへの差し替えを行うケースもあるようです。

- PCに感染するマルウェアのみならず、そういった不審なサイトへのリンクを含むコンテンツに引っかかることがないようにアンチウイルスやUTMによる防御は確実に行うべきでしょう。

マイナビニュース

【レポート】
SEOポイズニングにPDFを用いた新手法とは?(前編)

[2015/07/10]

今日、Webサイトを持っている企業はどこもGoogle検索結果の上位に表示されることがいかに重要かを認識しているはずだ。そのためにさまざまな検索エンジン最適化(SEO)テクニックが考案されており、サイト管理者はこれらをPageRankの上位になるためのキーとなる技術として利用している。

Google検索で上位に表示されるためには、コンテンツが特定の検索キーワードに対して関連性が高いということ、評判が良く関連性があるWebサイトに少しでも多くリンクされること、この2つが重要となる。

【レポート】
SEOポイズニングにPDFを用いた新手法とは?(後編)

[2015/07/13]

今日、Webサイトを持っている企業はどこもGoogle検索結果の上位に表示されることがいかに重要かを認識しているはずだ。そのためにさまざまな検索エンジン最適化(SEO)テクニックが考案されており、サイト管理者はこれらをPageRankの上位になるためのキーとなる技術として利用している。

前編で触れたクローキングの最後のステップとして、疑っていないユーザーがPDFのリンクをクリックした際に、不正なWebサイトにリダイレクトする。

ソフォスは、このテクニックはさまざまな目的に利用できると見ている。その1つが、マルウェアの散布。しかし、この手法が利用されているのを確認できたのは、"binary trading(バイナリー取引)"サービスのプロモーションを図るマーケティングキャンペーンのみだという。

IT用語辞典 e-Words

SEOポイズニング【 SEO poisoning 】

SEOポイズニングとは、検索エンジンの検索結果ページの上位に、コンピュータウイルスなどが含まれる悪質なWebサイトがリストされてしまう問題。

悪質サイトが人気の高い検索キーワードに対して検索エンジン最適化（SEO：Search Engine Optimization）を行うことにより、検索結果が汚染（poisoning）されてしまうことからこのように呼ばれる。

検索エンジンのユーザが特に悪質サイトとは関係の無い一般的なキーワードで検索を行うと、SEOで上位を獲得した悪質サイトが通常のサイトと並んで表示される。悪質サイトと気付かずにこれを訪問してしまうと、中に仕込まれていた悪意のあるソフトウェア（マルウェア）が起動し、ウイルスの感染やプライバシー情報の詐取、ローカルファイルの破壊などの攻撃を受けてしまう。

検索エンジン側では、Webサイトの情報を収集（クロール）する際にマルウェアが含まれているかどうかをチェックしたり、悪質なサイトを発見したら検索結果に載らないよう当該アドレスをブラックリストに載せるといった対策を行っている。

しかし、悪質サイトの側も、スクリプトが検知されないよう巧妙に隠したり、閉鎖されても別のホスティングサービスを利用してすぐに復活したりと対抗策を打ってくるため、「いたちごっこ」状態で対策が追いつかない実情がある。

●東京大学マルウェア感染被害、最大3万6千件の個人情報が流出

http://japan.cnet.com/news/business/35067514/
http://internet.watch.impress.co.jp/docs/news/20150716_712038.html

このニュースをザックリ言うと・・・

- 7月16日（日本時間）、東京大学から、同大学内の業務用PCがマルウェアに感染し、個人情報流出の被害が発生していたことが発表されました。

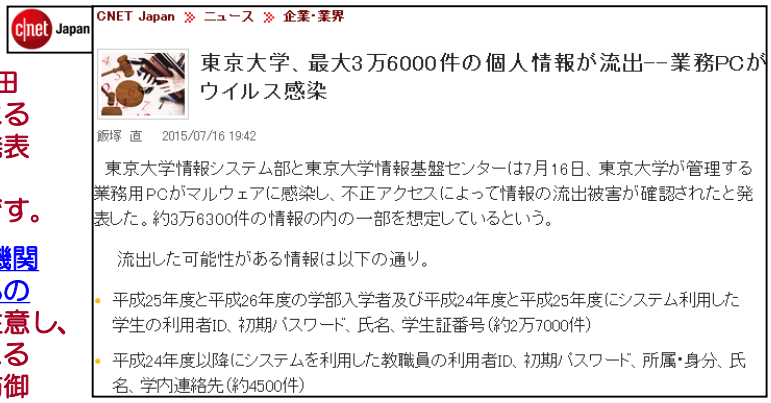
- 発表によると、6月30日に同大学内のメールサーバの設定が変更されていたことが確認され、調査の結果、業務用PCに保存されていた学内向けサービスの業務用アカウントが流出し、さらに当該PCや当該サービスのサーバに保存されていた情報も流出した可能性があるとされています。

- 流出した可能性がある個人情報は、「2013年度・2014年度の学部入学者および2012年度・2013年度にシステムを利用した学生の利用者ID・初期パスワード・氏名・学生証番号」約27,000件をはじめ、教職員・サーバ管理担当者のアカウント・個人情報を含む計約36,300件とされています。

AUS便りからの所感等

- 大学における個人情報流出事件は、6月に早稲田大学において、今回と同様のマルウェア感染による手口により、約3300件の流出があったことが発表されたばかりであり、この他、大手大学以外においても同様の被害発生が発表されているようです。

- 標的型攻撃のターゲットになるのは企業･政府機関・自治体そして大学等、特定の業種に限られるものではなく、そして大手中小の区別もないことに注意し、また、PCへのアンチウイルス導入と、UTMによる不正な通信の出入りの遮断といった、多面的な防御策をとることが肝要です。


CNET Japan » ニュース » 企業･業界

東京大学、最大3万6000件の個人情報が流出--業務PCがウイルス感染

飯塚 直　2015/07/16 19:42

東京大学情報システム部と東京大学情報基盤センターは7月16日、東京大学が管理する業務用PCがマルウェアに感染し、不正アクセスによって情報の流出被害が確認されたと発表した。約3万6300件の情報の内の一部を想定しているという。

流出した可能性がある情報は以下の通り。

- 平成25年度と平成26年度の学部入学者及び平成24年度と平成25年度にシステム利用した学生の利用者ID、初期パスワード、氏名、学生証番号（約2万7000件）
- 平成24年度以降にシステムを利用した教職員の利用者ID、初期パスワード、所属･身分、氏名、学内連絡先（約4500件）

●Flash Player、脆弱性の発覚とセキュリティアップデート相次ぐ

http://www.itmedia.co.jp/enterprise/articles/1507/13/news040.html
http://www.itmedia.co.jp/enterprise/articles/1507/15/news057.html

このニュースをザックリ言うと・・・

- 7月8日（米国時間）にセキュリティアップデート18.0.0.203（Windows版･以下同様）がリリースされたばかりのFlash Playerに、新たな脆弱性が存在することが同11日にAdobe社によって発表されました。

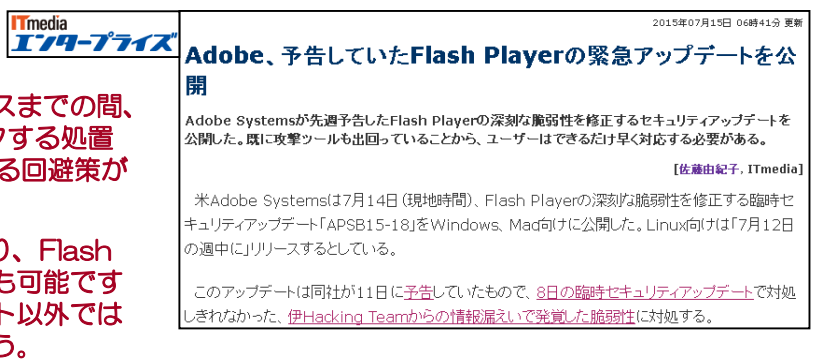
- 18.0.0.203で修正された脆弱性のいくつかは、Hacking Team社から流出した脆弱性情報から発覚したもの（AUS便り2015/07/13号参照）ですが、流出した情報にまだ未修正だった別の脆弱性を攻撃するコードが存在していた他、実際に攻撃が行われていることも明らかになっています。

- Adobe社は「12日の週(12～18日)中に緊急アップデートを行う」と予告、同14日には対策版となる18.0.0.209がリリースされています。

AUS便りからの所感等

- 7月11日の発表から18.0.0.209のリリースまでの間、Firefoxでは一時的にFlash Playerをブロックする処置をとった他、各所でFlash Playerを無効化する回避策が呼びかけられていた模様です。

- ブラウザによっては、設定やアドオンにより、Flashコンテンツを再生するサイトを制限することも可能ですので、よく調査の上、本当に必要となるサイト以外では無効にすること等を今後も検討すべきでしょう。


2015年07月15日 06時41分 更新

Adobe、予告していたFlash Playerの緊急アップデートを公開

Adobe Systemsが先週予告したFlash Playerの深刻な脆弱性を修正するセキュリティアップデートを公開した。既に攻撃ツールも出回っていることから、ユーザーはできるだけ早く対応する必要がある。

[佐藤由紀子，ITmedia]

米Adobe Systemsは7月14日（現地時間）、Flash Playerの深刻な脆弱性を修正する臨時セキュリティアップデート「APSB15-18」をWindows、Mac向けに公開した。Linux向けは「7月12日の週中に」リリースするとしている。

このアップデートは同社が11日に予告していたもので、8日の臨時セキュリティアップデートで対処しきれなかった、伊Hacking Teamからの情報漏えいで発覚した脆弱性に対処する。

- 最も重要なのはセキュリティアップデートの適用であることを念頭に置き、その上で、特にアップデートリリースまでのタイムラグにおける攻撃からの防御として、前述した回避策と、アンチウイルス・UTMの導入とを併用するのが良いでしょう。