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。

●Dell社製PCに不審なルート証明書、フィッシング悪用の恐れも

http://www.itmedia.co.jp/enterprise/articles/1511/24/news048.html
http://www.itmedia.co.jp/enterprise/articles/1511/25/news055.html
http://www.symantec.com/connect/ja/blogs/dell-edellroot

このニュースをザックリ言うと・・・

- Dell社製のノートPC等において、同社が独自に発行したルート証明書(※)（eDellRootおよびDSDTestProvider）がプリインストールされていることが11月になり複数報告されています。
- このルート証明書は同社アプリケーションのために発行されたものですが、各PCには共通した秘密鍵が保存されている模様で、攻撃者がこの秘密鍵を用いた署名を行うことにより、不正なWebサイトによる「中間者攻撃」が行われる可能性も指摘されています。
- Dell社では11月26日（日本時間）までに、当該証明書を完全に削除するソフトウェアアップデートをリリースする等の対応を行っています。

AUS便りからの所感等

- 同様の不正なルート証明書の存在は、2月にもLenovo社製のノートPCで発覚しています。
- 中間者攻撃、即ちユーザとサーバの間で「攻撃者が通信の傍受や改ざんを行う攻撃」において、秘密鍵によって署名された証明書を用いたサーバに誘導されても検知できない可能性があることが問題となっています。
- 該当するPCを利用しているユーザについては、同社からの情報とPC上に当該証明書がプリインストールされているかを確認の上、確実に削除を行うようにしてください。
- なお、ブラウザやUTMのアンチフィッシング機能においては、今後該当する秘密鍵で署名された証明書や中間者攻撃を行っているような不正なサーバへのアクセスを検知・遮断できるようになることも考えられます。

ITmedia エンタープライズ

2015年11月24日 07時46分 更新

DellのPCに不審なルート証明書、LenovoのSuperfishと同じ問題か

Dellのマシンにプリインストールされている自己署名ルート証明書の「eDellRoot」について、危険を指摘する声が相次いでいる。

[鈴木聖子, ITmedia]

米Dellのノートに不審なルート証明書がプリインストールされているのを見付けたというユーザーの報告が、11月22日ごろにかけて相次いだ。Lenovoのコンピュータで発覚した「Superfish」と同様に、偽の証明書発行に利用され、HTTPS通信に割り込む攻撃に悪用される恐れも指摘されている。

2015年11月25日 07時41分 更新

Dell、ルート証明書の脆弱性で対応表明　別の問題発覚

Dellはシステムから「eDellRoot」を恒久的に削除する方法について説明。一方、米CERT/CCは、Dellの別のルート証明書「DSDTestProvider」に関する脆弱性情報も公開した。

[鈴木聖子, ITmedia]

米DellのPCにルート証明書と秘密鍵が搭載されているのが見つかり、攻撃に悪用されかねないと指摘された問題で、Dellは11月23日、この証明書が脆弱性を生じさせていることを認めて対応を表明した。一方、米カーネギーメロン大学のCERT/CCは24日、この問題のほか、Dellの別のルート証明書と秘密鍵の問題についても脆弱性情報を出している。

シマンテック公式ブログ

0
0 Votes

Dell のコンピュータで、自己署名されたルート証明書 eDellRoot が見つかる

Dell 社のコンピュータの一部で **eDellRoot** という名前のルート証明書がインストールされていることが確認されました。攻撃者は **SSL/TLS** 証明書に署名して正規のソースであるかのように偽装したり、中間者攻撃を実行したりできる恐れがあります。

投稿者: **Symantec Security Response** シマンテック従業員

作成日 25 Nov 2015

IT用語辞典 e-Words

（※）ルート証明書【 root certificate 】

ルート証明書とは、デジタル証明書を発行する認証局が、その正当性を証明するために自ら署名して発行するデジタル証明書。SSLなどで暗号通信を利用する必要のあるOSやWebブラウザには、大手認証局のルート証明書があらかじめ組み込まれており、受信した証明書が正当なものかどうかを確認するための信頼の基点となる。

Webサイトなどと暗号通信を行う時に相手の送ってきたデジタル証明書が正当なものか調べるには、証明書の発行機関を調べ、その機関が信用できるかどうかを調べるために発行機関の証明書を調べ、という具合に遡っていく。このとき、信頼できる認証局が自己署名した証明書をあらかじめ保持しておき、遡った結果この認証局に行き当たったら証明書は信頼できるとみなすことができる。この信頼の大元として使われる証明書をルート証明書という。

ルート証明書はユーザが必要に応じて自分でインストールすることもできるが、通常は実績ある大手の認証機関のルート証明書がWebブラウザなどに組み込まれており、ユーザが意識することは少ない。ルート証明書を発行した認証局をルート認証局（ルートCA）と呼ぶことがある。

●Linuxを狙うランサムウェアの被害拡大

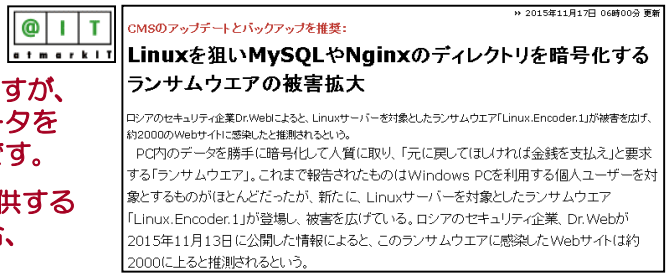
http://www.atmarkit.co.jp/ait/articles/1511/17/news048.html

このニュースをザックリ言うと・・・

- 11月13日（日本時間）、ロシアのセキュリティ企業Dr.Web社より、Linuxサーバを対象としたランサムウェア「Linux.Encoder.1」による被害が広がっているとして警告が出されました。

- Linux.Encoder.1は、Magento（ECサイト構築プラットフォーム）やWordPress（ブログツール）のようなコンテンツ管理システム（CMS）の古いバージョンに存在する脆弱性を突いてサーバに侵入、Webサーバプロセスを実行しているユーザ（www-data）の権限でサーバ上の様々なファイルを暗号化し、復号のための身代金として1ビットコインを要求する脅迫文を出力するとのことです。

- Dr.Web社によると、サーチエンジンによってこの脅迫文の検索を行った結果から、約2,000のWebサイトがLinux.Encoder.1に感染しているものと推測しています。



» 2015年11月17日 06時00分 更新

CMSのアップデートとバックアップを推奨：

Linuxを狙いMySQLやNginxのディレクトリを暗号化するランサムウエアの被害拡大

ロシアのセキュリティ企業Dr.Webによると、Linuxサーバーを対象としたランサムウエア「Linux.Encoder.1」が被害を広げ、約2000のWebサイトに感染したと推測されるという。

PC内のデータを勝手に暗号化して人質に取り、「元に戻してほしければ金銭を支払え」と要求する「ランサムウエア」。これまで報告されたものはWindows PCを利用する個人ユーザーを対象とするものがほとんどだったが、新たに、Linuxサーバーを対象としたランサムウエア「Linux.Encoder.1」が登場し、被害を広げている。ロシアのセキュリティ企業、Dr.Webが2015年11月13日に公開した情報によると、このランサムウエアに感染したWebサイトは約2000に上ると推測されるという。

AUS便りからの所感等

- 今回については幸いにもデータの復旧は可能とのことですが、本来であれば、ランサムウェアによって暗号化されたデータを常に復旧できるとは限らないことは度々述べている通りです。

- Linuxサーバにおいては、ディストリビューションが提供するパッケージ以外からソフトウェアをインストールした場合、セキュリティアップデートをyum（CentOS, RHEL）やapt（Debian, Ubuntu）によって適用できず、全て手動で行う必要があることに特に注意すべきです。

- サーバの前面にUTMを設置する等でWebアプリケーションファイアウォール（WAF）を有効にすることにより、マルウェアが侵入するための不正なリクエストを事前に遮断できる可能性もありますが、やはり各種ソフトウェアのアップデート、および万が一の感染時の復旧のためのシステム・データの随時のバックアップが大切と言えるでしょう。

●Androidアプリ内のPNG画像にマルウェアを仕込んでアンチウイルスソフトを回避する手口が発見される

http://gigazine.net/news/20151125-android-malware-png/

このニュースをザックリ言うと・・・

- 11月23日（現地時間）、セキュリティ研究者のLukas Stefanko氏より、新たな手口によってマルウェアが仕込まれたAndroidアプリの存在が確認されたとブログで発表されました。

- 同氏の調査によれば、マルウェアの本体はアプリに含まれる画像データ内にBase64（バイナリデータをテキストで表現するためのエンコード形式）でエンコードされた状態で存在していたとのことで、オンラインでウイルススキャンを行う「VirusTotal」では記事を投稿した時点で全く検出されなかったとのことです。

- アプリの実行により、画像データ内からマルウェアの本体を取り出して実行し、Google Play Storeやオンラインバンキングサイトへのアクセス時にアカウント情報を奪取する他、アンインストールがしにくいものとなっている模様です。

2015年11月25日 20時00分00秒

Androidアプリ内のPNG画像にマルウェアを仕込んでアンチウイルスソフトを回避する手口が発見される

Androidアプリに含まれるPNG画像に、暗号化した「トロイの木馬」を埋め込み、アンチウイルスソフトを回避してしまうAndroidアプリが発見されました。

Android Malware: Android malware drops Banker from PNG file
http://b0n1.blogspot.jp/2015/11/android-malware-drops-banker-from-png.html

マルウェアに関して研究しているLukas Stefankoさんは、PNG画像のファイルデータの中にBase64エンコード方式のトロイの木馬が埋め込まれているAndroidアプリを発見したそうです。ファイル内にマルウェアが潜んでいるのはよくある手口ですが、画像に暗号化したウイルスを仕込む方法は非常に珍しいとのこと。
マルウェアが埋め込まれたアプリを、40種類以上のウイルス対策製品を使用してファイルを検査する無料オンラインサービス「VirusTotal」でスキャンしたところ、ほとんどのウイルス対策製品はウイルスの埋め込まれたPNG画像を検出できなかったことが明らかになっています。

AUS便りからの所感等

- 問題となったアプリはGoogle Playにアップロードされたものではない模様ですので、そういった信頼されたサイトからのみダウンロードすることが自衛のためには重要でしょう。

- その後のVirusTotalのスキャン結果を見る限りでは、一部アンチウイルスソフトではマルウェアを検出しつつあり、今後も各社での対応は進むものと見られます。

- VPN機能を提供するUTM配下での利用により、こういった不審なアプリファイルのダウンロードを食い止めることも期待できるでしょうが、最低限、スマートフォンにアンチウイルスソフトをインストールすることを推奨します。