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。

●ヤマダ電機通販サイトからカード情報約37,000件流出…不正アクセスでWebアプリ改ざん

https://www.itmedia.co.jp/news/articles/1905/29/news114.html
https://www.yamada-denki.jp/information/190529/

このニュースをザックリ言うと･･･

- 5月29日（日本時間）、ヤマダ電機より、同社通販サイト「ヤマダウェブコム」「ヤマダモール」が不正アクセスを受け、利用者のクレジットカード情報が流出した可能性があると発表されました。

- 発表によれば、流出の被害を受けたとされるのは、3月18日～4月26日の間に同サイトで新規登録または情報変更した最大37,832件のカード情報（カード番号、有効期限およびセキュリティコード）とのことで、一部悪用が確認されているとのことです。

- 不正アクセスにより、上記の期間にWebサイトの決済アプリケーションが改ざんされていたことが流出の原因としており、同社では4月16日に流出の可能性を把握、その後調査を経て同26日にサイトでのカード登録等を停止したとのことです。

AUS便りからの所感等

- Webアプリケーションの改ざんにより、「カード情報入力画面に入力した内容が外部に送信されるようになっていた」もしくは「偽のカード情報入力画面に誘導するようになっていた」可能性が考えられます。

- クレジットカード情報（あるいはアカウント・個人情報）を詐取する手口は様々ですが、今回のように実際の決済画面表示時において改ざんを行うケースは、フィッシングメールやマルウェア感染によって誘導するケースに比べてユーザ側での対策が難しく、より確実に情報を詐取できる可能性が高いでしょう。

- クライアントPCのみならずサーバ上においても、脆弱性を突かれることのないようWebアプリケーション等を最新のバージョンに保つことは重要ですし、加えてサーバの設定やソリューションの導入等により、適切なアクセス制限からアプリやコンテンツの改ざん検知あるいは内部からの不正な通信の遮断に至るまで、様々な対策を実施するよう考慮すべきです。

ITmedia NEWS

ヤマダ電機、不正アクセスで顧客のクレジットカード情報流出　最大3万7000件

◎ 2019年05月29日 17時28分 公開　　[井上輝一，ITmedia]

印刷　5584　Share　B!　54

ヤマダ電機は5月29日、同社が運営するオンラインストア「ヤマダウェブコム」「ヤマダモール」が不正アクセスを受け、約3万7000件のクレジットカード情報が流出した可能性があると発表した。一部は不正利用された可能性もあるという。

【修正：2019年5月29日午後6時50分　記事タイトルと第1段落の記述を一部修正しました】

流出した可能性があるのは、2019年3月18日～4月26日の期間に同サイトで新規クレジットカード登録や登録変更をした最大3万7832件の顧客情報。クレジットカード番号、有効期限、セキュリティコードが流出し、一部顧客のクレジットカード情報が不正利用された可能性があることを確認しているという。

同社のペイメント（決済）アプリケーションが第三者に改ざんされていたことが、流出の原因とみている。

現在、クレジットカード会社と連携し、流出した可能性のあるクレジットカードによる取引のモニタリングを継続しているとした上で、「見に覚えのない請求がないか、いま一度確認してほしい」と顧客に呼びかけている。また、希望者には無料でカードが再発行されるという。

ヤマダ電機は流出の可能性について4月16日に把握し、調査を経て26日に同サイト上でのクレジットカード登録、登録変更を停止した。同日、第三者調査機関による調査を開始し、5月20日に完了。同社は「正確な状況を把握しない段階で公表することはかえって混乱を招くため、第三者調査機関の最終報告書をもって報告することにした。情報公開が遅れたことを深くおわびしたい」としている。

YAMADA

2019年5月29日

お客様各位

株式会社　ヤマダ電機

弊社が運営する「ヤマダウエブコム・ヤマダモール」への不正アクセスによる個人情報流出に関するお詫びとお知らせ

このたび、弊社が運営する「ヤマダウエブコム・ヤマダモール」におきまして、第三者による不正なアクセスを受け、クレジットカードの情報が最大37,832件流出した可能性があることが2019年4月16日に判明いたしました。
お客様をはじめ、関係者の皆様に多大なるご迷惑およびご心配をおかけする事態となりましたこと、深くお詫び申し上げます。

弊社では、今回の事態を厳粛に受け止め、再発防止のための対策を講じてまいります。
お客様をはじめ関係者の皆様には重ねてお詫びを申し上げますとともに、本件に関する概要につきまして、下記の通りご報告いたします。

不正アクセスの可能性が疑われたため、調査を経て2019年4月26日時点で　「ヤマダ ウエブコム・ヤマダモール」での新規クレジットカード登録、及びクレジットカード登録の変更を停止いたしました。
同時に、第三者調査機関「P.C.F.FRONTEO株式会社」による調査も開始いたしました。
2019年5月20日、調査機関による調査が完了し、2019年3月18日～2019年4月26日の期間に「ヤマダウエブコム・ヤマダモール」で新規クレジットカード登録、及びクレジットカード登録の変更をされたお客様のクレジットカード情報が流出し、一部のお客様のクレジットカード情報が不正利用された可能性があることを確認いたしました。
以上の事実が確認できたため、発表させていただきます。

・個人情報流出状況
(1)原因
第三者によって「ヤマダウエブコム・ヤマダモール」に不正アクセスされ、ペイメントアプリケーションの改ざんが行われたため

(2)個人情報流出の可能性があるお客様
2019年3月18日～2019年4月26日の期間中に「ヤマダウエブコム・ヤマダモール」において新規クレジットカード登録、及びクレジットカード登録の変更をされたお客様最大37,832名で、流出した可能性のある情報は以下のとおりです。
【流出した可能性のある情報】
・クレジットカード番号
・有効期限
・セキュリティコード

●マルウエアが含まれたショートカットファイルをダウンロードさせる攻撃、JPCERT/CCが紹介

https://blogs.jpcert.or.jp/ja/2019/05/darkhotel_lnk.html

このニュースをザックリ言うと・・・

- 5月29日（日本時間）、JPCERT/CCより、4月～5月に日本の組織に対して送信された標的型攻撃メールについて解説されています。

- 攻撃メールに添付されているショートカットファイル（.lnk）を開くことにより、外部からのHTMLファイルのダウンロード、スクリプトの実行等の複数の手順を経て、.lnkファイルに埋め込まれていたダウンローダー等を展開して実行する仕組みになっているとのことです。

- JPCERT/CCでは、ダウンローダーが最終的にマルウェア等を取得する様子までは確認できなかったものの、今度も同様の攻撃が行われる可能性があるとして、注意喚起を行っています。

AUS便りからの所感等

- .lnkファイルは単にPC上のファイルの場所だけではなく、実行するコマンドやパラメータ等の指定も可能なため、不正な.lnkファイルからマルウェアに感染させようとする手口自体は昔から知られています。

- ダウンローダーは.lnkファイル内にそのままのバイナリ形式で埋め込まれていたわけではなく、自己展開形式の.exeファイルに格納された上で、その.exeファイルをテキスト形式にエンコードした状態で埋め込まれ、さらにそれを展開するまでに複数の手順を経ることにより、アンチウイルスによる検出が行われないよう工夫していたとみられます（このような手口もまた昔から存在します）。

- いずれにせよ不審なメールに添付されている.lnkファイル（zip等に含まれるものも含む）は安易にクリックしないよう十分注意し、アンチウイルスやUTMによる防御を十分に固めるようにしましょう。

●Windowsに3つの未修正脆弱性、匿名のセキュリティ研究者発表

https://news.mynavi.jp/article/20190529-832680/

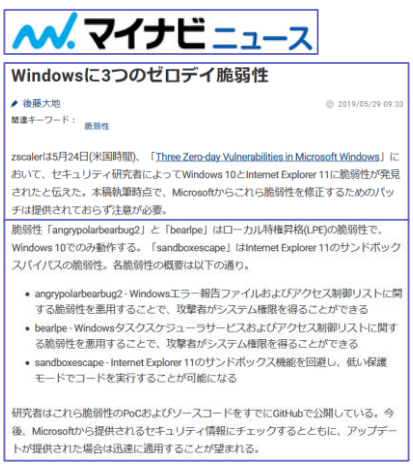
このニュースをザックリ言うと・・・

- 5月24日（米国時間）、セキュリティベンダーのzscaler社より、Windows 10およびInternet Explorer（IE）に存在する未修正の脆弱性3点について同社のブログにて取り上げられています。

- Windows 10の脆弱性（angrypolarbearbug2, bearlpe）は攻撃者がシステム権限を奪取し、PCを乗っ取る等が可能とされており、IEの脆弱性（sandboxescape）はより低い保護モードでのコードの実行が可能とされています。

- これらの脆弱性は「SandboxEscaper」を名乗る匿名のセキュリティ研究者が発表しており、同時に攻撃コードが公開されています。

AUS便りからの所感等



- Windowsの脆弱性はタスクマネージャーのジョブファイルの処理等に存在するもので、10より前の7や8.1では影響はないものの、PC上で不正なコマンドを実行するよう誘導する必要があるとみられることから、この脆弱性を悪用するマルウェアはメールに添付される形で拡散することが考えられます。

- zscaler社が提供するプロダクトではこれらの脆弱性を突く攻撃コードの検知に対応しているとのことで、各社アンチウイルス等においても同様に対応が進むとみられますので、パッチが提供されるまでの間に攻撃を受けないためにも確実に防御を固めておくことが肝要です。