— AUS（アルテミス・ユーザ・サポート）便り 2018/05/28号 —
https://www.artemis-jp.com

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。

●日本人の個人情報のべ2億件以上流出、中国のネット上でわずか17,000円で売買

http://www.itmedia.co.jp/business/articles/1805/17/news117.html
https://www.fireeye.com/blog/jp-threat-research/2018/05/japan-pii-finding.html

このニュースをザックリ言うと・・・

- 5月17日（日本時間）、国内セキュリティベンダーのファイア・アイ社より、日本人ユーザの個人情報が中国のアンダーグラウンド・フォーラム（反社会的なWeb掲示板）で取引されていたとする調査結果が発表されました。

- 発表によれば2017年12月頃、掲示板サイトに「日本人の個人情報を収録したデータセットを販売する」との広告が掲載されているのを発見したとのことです（現在この広告は取り下げられています）。

- データセットに含まれていたのは、一般人の氏名・メールアドレス・アカウント情報（ID･パスワード）・生年月日・電話番号・住所等のべ2億件以上で、1000人民元（1万7000円）程度で取引されていたとのことです。

AUS便りからの所感等

- データセットには情報源とされる日本の企業名や取得した時期も記されており、発表では流出元として、日本の食品ECサイト、アダルトサイトおよびゲーム関連サイト等が挙げられている一方、偽のメールアドレスや重複も一定数あったとのことです。

- 同社では、「流出した個人情報は過去のものが多く、大規模な攻撃が行われることはない」と予想する一方、「当時のID･パスワードを再利用している企業や個人は、迷惑メール、マルウェア、詐欺などの対象になる可能性がある」ことを指摘しています。

- 流出元の具体的な名前が挙げられていないこともあり、今後ユーザが自分たちのアカウント情報がこれに含まれているか調べられるようになるかは未知数ですが、万が一アカウント認証情報の流出が確認、あるいはその可能性が考えられる場合は、必ずパスワードの変更を行えるよう、所有する全てのアカウントについて備えておくべきでしょう。

ITmediaビジネス ONLINE

たったの1万7000円：

日本人の個人情報2億件、中国の闇サイトで販売か

2018年05月17日 18時20分 公開　[濱口翔太郎，ITmedia]

印刷　通知　185　255　B! 10

中国のアンダーグラウンド・フォーラム（反社会的なWeb掲示板）で、2億件以上の日本人の個人情報が取引されていた――セキュリティ企業のファイア・アイは5月17日、こんな調査結果を明らかにした

同社は2017年12月ごろ データセットを販売す メントを残していたと

データセットに含ま （ID・パスワード）、 データセットは、1000

ファイア・アイは具体的な企業名を伏せたが、流出元として日本の食品EC（インターネット通販）サイト、アダルトサイト、ゲーム関連サイトなどを挙げた。過去の大規模情報漏えい事件で流出したデータも大量に含まれていたという。

日本人の個人情報流出 - 背景

- 2017年12月初旬、中国の脅威アクターが日本人の個人情報が含まれたファイルをアンダーグラウンド・フォーラム上で販売
- ファイルに含まれていたデータは2億件以上、1,000人民元（150.96米ドル）の価格で販売されていた
- 小売、食品、飲料、金融、エンターテインメント、交通など、11件～50件の国内Webサイトから盗まれたと考えられる
- サンプルには重複値やダミーデータも含まれていたが、データ自体は本物であると考えられる

流出の経緯（＝ファイア・アイ調べ）

FireEye

日本人の個人情報2億件以上が含まれたファイルを 中国の脅威アクターが販売目的で広告掲載

2018年5月17日 | by FireEye

概要

- FireEye iSIGHTインテリジェンスは2017年12月初旬、ある脅威アクターが、個人情報を収録したデータセットを販売する目的で広告を掲載しているのを発見しました。このデータセットは国内複数のWebサイトのデータベースから抽出された、本物のデータであるとファイア・アイは分析しています。
- 情報の流出源が非常に多く、個人情報の種類も多岐にわたることから、このデータは、特定の組織への標的活動ではなく、日和見的な不正アクセスによって取得されたと考えられます。
- この脅威アクターは、少なくとも2013年9月より、中国のアンダーグラウンド・フォーラム上でWebサイトのデータベースを積極的に販売しており、中国浙江省在住の個人との関連が疑われています。

はじめに

2017年12月、中国のアンダーグラウンド市場において、ある脅威アクターが、個人情報を収録したデータセットを販売する目的で広告を掲載しているのが発見されました。データセットには、氏名、認証情報（ID・パスワード）、メールアドレス、生年月日、電話番号と住所が含まれていました。脅威アクターはデータセットに一意の認証情報セットが2億件収録されており、国内で人気の複数のWebサイトのデータベースから抽出したと謳っています。また、このデータは、1,000人民元（150.96米ドル）の価格で販売されていました。データそのものは、小売、食品、飲料、金融、エンターテインメント、交通など、さまざまな業界のWebサイトから盗まれたと考えられます。各フォルダのラベルには、データが2016年の5月から6月に取得されたものと示すものもあれば、2013年の5月と7月に取得されたことを示す日付も観察されています。

●Linuxベースのルータ やNASに感染するマルウェア「VPNFilter」、54カ国50万台に感染か

https://internet.watch.impress.co.jp/docs/news/1123623.html

このニュースをザックリ言うと・・・

- 5月23日（現地時間）、Cisco社のセキュリティ部門TalosやFortinet社およびSymantec社等より、54カ国で50万台以上ものネットワーク機器（ルータやNAS）等に感染しているマルウェア「VPNFilter」についての注意喚起が相次いで出されました。

- VPNFilterはLinuxベースの機器に感染すると、再起動時にも再度自身が実行されるようフラッシュメモリを書き換えた上で、外部の司令サーバからパケット監視・Tor通信等を行うプログラムをダウンロードしてボットネットを構築するとされています。


INTERNET Watch

Linuxベースのルーターや NASに感染するマルウェア「VPNFilter」、54カ国50万台に感染か、Cisco Talos報告

岩崎 宰守　2018年5月24日 13:21

ツイート　リスト　いいね！100　シェア　B! 29　Pocket　116

米Ciscoのセキュリティ部門Talosは23日、モジュール化されたフレームワークを持つ高度なマルウェア「VPNFilter」が、54カ国で50万台以上のネットワーク機器などへ感染していることを報告。注意を喚起している。

VPNFilterは、モジュール化されたフレームワークにより、3つのステージへ拡張を行う高度なマルウェア。ステージ1では、Linuxベースのファームウェアを実行しているデバイスへ感染し、いくつかのCPUアーキテクチャー向けにコンパイルを実行。次に機器が再起動されても継続して活動できるよう、フラッシュメモリ内に自身を格納する。また、ステージ2へ移行可能なC2サーバーを探索する。

ステージ2では、作業環境を設定し、C2サーバーに接続。取得されたコマンドの実行やファイルのダウンロード、デバイスの管理などを行う。また、ステージ2のプラグインとして機能するステージ3のモジュールには、プロトコルの監視を行うパケットスニッファー、Tor通信用モジュールなどが存在しているという。

AUS便りからの所感等

- 3月下旬に情報通信研究機構（NICT）やNTT東西各社がルータへの攻撃に関する注意喚起を出しており（AUS便り 2018/04/02号参照）、今回の攻撃はそのターゲットが世界中へ拡大したものとされています。

- Symantec社の発表では、3月の攻撃と同様、管理画面にログインするパスワードが初期状態から変更されていなかった機器を狙った感染であることが指摘されており、また万が一感染した場合、機器を再起動してもマルウェアが残り続けるため、工場出荷時の状態にリセットすることにより駆除することを推奨しています。

- ユーザが頻繁に触ることのないネットワーク機器・IoT機器について管理の意識が及びにくいことに十分注意し、設置の際には必ずパスワードを設定する等、以後も確実に管理を行う体制を整え、また可能な限り前面にUTM等を設置し、第三者から本来アクセスされるべきでないポートについてのフィルタリングと外部への不正通信を遮断できるネットワーク構成とすることが望ましいです。

●メニコン子会社、カード情報約3400件流出…668万円不正使用

https://www.nikkei.com/article/DGXMZO30643680X10C18A5CN8000/

このニュースをザックリ言うと・・・

- 5月17日（日本時間）、コンタクトレンズ大手のメニコン社より、子会社ダブリュ・アイ・システム社が運営するECサイト「A-Web倶楽部」が不正アクセスを受け、最大3412件の顧客のクレジットカード情報が流出したと発表されました。

- 流出したのは2017年12月17日～2018年3月27日の間に同サイトの宅配サービスを利用したユーザの会員名・カード番号・有効期限の情報で、うち27件が不正利用され、約668万円の被害が出ているとのことです。

- 3月に不正使用の可能性について指摘を受け調査したことにより発覚、現在サイトは閉鎖されています。

AUS便りからの所感等

- カードの不正利用があったとのことで、セキュリティコードも流出した可能性がありますが、現時点では不明です。

- Webアプリケーションの脆弱性を突いた不正アクセスとされており、こちらも詳細は発表されていませんが、近年発生したクレジットカード情報流出で悪用された脆弱性としては、「Apache Struts2」の脆弱性（AUS便り 2017/11/27号参照）等が知られています。

- Webアプリケーションの脆弱性を狙う攻撃の中には、明らかに攻撃であると推測できるアクセスのパターンによるものも存在しますので、脆弱性への根本的対策としてWebアプリケーション自体の修正は決して怠ってはならないことですが、攻撃とみられるアクセスを検出・遮断するため、Webサーバ自体あるいはUTMによるWAF（Webアプリケーションファイアウォール）の設置による防御も重要な顧客の機密情報等を守るためには検討に値するでしょう。


日本經濟新聞

メニコン子会社、カード情報流出　668万円不正使用

中部 社会

2018/5/17 18:48

保存　共有　印刷　その他

コンタクトレンズ大手のメニコン（名古屋市）は17日、子会社の通販サイトが外部から不正アクセスを受け、最大約3400件の顧客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。2日時点で27件、計約668万円分のカードの不正使用が確認された。警視庁に被害を相談している。

メニコンによると、子会社「ダブリュ・アイ・システム」（東京・豊島）が運営する通販サイト「A—Web倶楽部」に対し、システムの脆弱性を突いた不正アクセスがあった。2017年12月17日～18年3月27日に同サイトで決済をした顧客のカード番号や有効期限など最大約3400件の情報が流出した可能性がある。

3月にカード会社から不正使用の可能性について指摘があり、メニコンが第三者機関に調査を依頼。5月2日にカード情報の流出や27件の不正利用が判明した。流出のあったサイトは現在、閉鎖されている。他の子会社が運営する通販サイトに対する不正アクセスは確認されていない。