— AUS（アルテミス・ユーザ・サポート）便り 2017/05/01号 —
http://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。

●ゴールデンウィークにおける情報セキュリティに関する注意喚起、IPA・JPCERT呼びかけ

https://www.ipa.go.jp/security/measures/vacation.html
https://www.jpcert.or.jp/pr/2017/pr170001.html

このニュースをザックリ言うと･･･

- 多くの企業が長期休暇となるゴールデンウィークを迎えるにあたり、4月21日（日本時間）にIPA、同24日にはJPCERT/CCより、情報セキュリティに関する注意喚起が出されています。

- システム管理者が長期間不在になることにより、ウイルス感染や不正アクセス等の被害が発生した場合に対処が遅れてしまう可能性、および従業員等が友人や家族と旅行に出かけた際の、SNSへの書き込み内容から思わぬ被害が発生、場合によっては関係者にも被害が及ぶ可能性を指摘しています。

- IPA・JPCERT/CCそれぞれの資料では、組織内のシステム管理者やユーザに対し、休暇前・休暇中および休暇明けにとるべき対策のポイントを挙げており、例えば、IPAでは管理者に対して、休暇前に「緊急連絡体制の確認」「使用しない機器の電源OFF」等、休暇明けに「パッチの適用」「アンチウイルス定義ファイルの更新」「サーバ等の各種ログの確認」を呼びかけています。

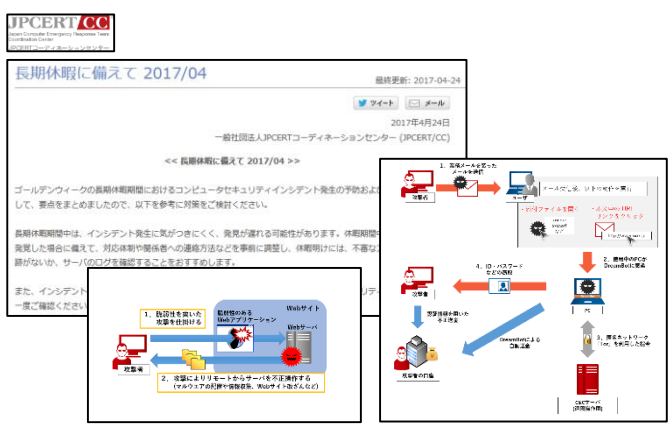
- またユーザに対しては、業務対応等の理由で機器やデータを持ち出す必要がある場合、休暇前の「持ち出しルールの確認と遵守」、休暇中の「厳重な管理」および休暇明け時にはやはり「パッチの適用」「アンチウイルスパターンファイルの更新」そして「持ち出した機器やUSBメモリ等のウイルスチェック」を行うよう呼びかけており、この他、家庭（プライベート）におけるインターネットの利用者の観点からも、無線LANやSNS利用等に関する注意点を挙げています。

AUS便りからの所感等

- セキュリティ機関の呼びかけは、情報システムとインターネットを組織内外で利用する者として、「普段から」セキュリティを意識した慎重な行動をとることを改めて示す以外にも、「いつもとは違う状況になる」ことで通常時には生じにくい様々な問題にも早く確実に対応することへの注意を促すものとなっています。

- 休暇期間中には、マルウェアが添付されたメールが全く新しい文面で拡散したり、あるいはマルウェアに感染したとかたって電話をかけさせる偽の警告が活発化したりする可能性も考えられますので、UTMによるネットワークの防御、ソフトウェアのアップデートやアンチウイルス等を用いてのPCの防御以外にも、全てのユーザに対する随時のセキュリティ教育や情報の共有がそういった攻撃による被害を最小限に抑えられるために大切なことと言えます。

- もしこのAUS便りを連休明けにご覧になったとしても、その時点で点検すべきことは多く存在しますので、以後も夏季・年末年始といった長期休暇に備えて、準備・点検を行うよう意識して頂ければ幸いです。



●ぴあのWebサイトから個人情報15万件流出か…カード不正利用630万円

http://www.nikkei.com/article/DGXLASDG25H6K_V20C17A4CR0000/

このニュースをザックリ言うと・・・

- 4月25日（日本時間）、チケット販売大手のぴあ社より、同社が運営委託を受けていたプロバスケットボール「Bリーグ」のチケットサイトおよびファンクラブサイトが不正アクセスを受け、個人情報147,093件（住所・氏名・ID・パスワード・メールアドレス他）が流出した可能性があると発表されました。

- セキュリティコードを含むクレジットカード情報32,187件も流出したとされ、既に197件・計630万円分のカードの不正利用が確認されているとのことです。

- 当該サイトで利用していた「Apache Struts2」に対し、3月上旬に発表されていた脆弱性を悪用して3月7日～15日の間に不正アクセスを受けていたことを確認しており、4月20日までにアップデートとWAF等による対策を行ったと発表しています（なお、同社が運営する「チケットぴあ」はStruts2を使用していないとのことです）。

AUS便りからの所感等


日本経済新聞

ぴあ、個人情報15万件流出か　カード不正利用630万円
プロバスケサイトにサイバー攻撃
2017/4/25 19:21

チケット販売大手のぴあは25日、同社がプラットフォームを提供し運営を受託しているプロバスケットボール・Bリーグのチケットサイトとファンクラブのサイトがサイバー攻撃による不正アクセスを受け、個人情報約15万件が流出した可能性があると発表した。約3万2千件のクレジットカード情報が含まれ、21日時点でカードの不正使用が197件、計約630万円分確認された。

ぴあはすでに警視庁に相談したとしている。

同社によると、流出した可能性があるのは2016年5月16日～17年3月15日に、Bリーグの会員に登録した顧客の個人情報約15万件。住所、氏名、電話番号、生年月日、メールアドレスなどの登録情報が含まれる。

- クレジットカード情報の流出、しかも保存が禁止されているセキュリティコードを含めての流出という、3月10日の都納税サイト等の件（AUS便り2017/3/13号参照）と同様の事態となり、被害を受けた2サイトの開発・運用を再委託していた外部業者がセキュリティコードを保存する仕様にしていたとされています。

- 事情は不明ですが、こういった重大な仕様のミスが起きてないか、委託する側も十分に確認する必要があり、万が一の流出で発生し得る損害額を鑑みるならば、決済代行業者との契約により、カード情報を自前で保持しないシステムとすることも重要です。

- Struts2の未修正の脆弱性を突いての不正アクセス事件は後を絶たず、特に今回の事件は3月7日という非常に早い段階から不正アクセスが発生していたとされており、Struts2を利用していて万が一アップデートしていなければ速やかに実施し、並行してUTMの設置によるWAF等の有効化により、今後の脆弱性の発表からアップデートまでの攻撃を緩和できる体制を作っておくことが肝要です。

●正規のAndroidアプリから200万人がマルウェアに感染

https://japan.zdnet.com/article/35100328/

このニュースをザックリ言うと・・・

- 4月24日（現地時間）、大手セキュリティベンダーのチェックポイント社より、Androidの公式アプリストア「Google Play」でダウンロードしたアプリからマルウェアに感染するケースが確認されているとして警告が出されています。

- 「FalseGuide」（偽ガイド）と呼ばれるマルウェアは、40種類以上のゲームの攻略法を解説するガイドアプリに仕込まれていたとされ、感染すると不正なポップアップ広告を表示する仕組みになっていたとのことで、アプリが登録されたのは少なくとも2016年11月まで遡るとみられ、200万人以上のユーザが感染の被害を受けたとされています。

- チェックポイント社では2月にFalseGuideについてGoogleに通知しており、現在問題となるアプリは削除されていますが、一度インストールしたら簡単にアンインストールできない仕組みになっているためか、依然一部のスマホ等でアプリが動作し、被害をもたらしている模様です。

AUS便りからの所感等


ZDNet Japan

人気ゲームのガイドアプリにマルウェア、多数のAndroidデバイスが感染--Check Point

Danny Palmer（ZDNet.com）翻訳校正：編集部 2017年04月26日 13時10分

多数のデバイスが、「Android」の公式アプリストアである「Google Play」からダウンロードしたマルウェアに感染していたことが明らかになった。

このマルウェアはボットネットを構築し、モバイル用のアドウェアを表示する。

「FalseGuide」（偽ガイド）と名付けられたこのマルウェアは、Check Pointのセキュリティ研究者が発見したもので、「Pokemon GO」や「FIFA Mobile」などを含む40種類以上の有名ゲーム用コンパニオンガイドアプリに隠されていた。もっとも古いものは、2017年2月14日からGoogle Playにアップロードされていたという。

- 今回のFalseGuideで確認された具体的な被害は不正なポップアップ広告ぐらいで、これで広告収入を得ることが目的だったとされている一方、ボットネットへの接続も行っており、指令により、デバイスを一斉に乗っ取られ、外部へのDDoS攻撃や、内部ネットワークへの侵入に悪用される可能性もあったと推測されています。

- これまでのスマホアプリからマルウェアに感染するケースは、非公式のアプリストア等からダウンロードする場合が主で、Google Playを利用する場合は安全と言う認識もされていましたが、今回のようにマルウェアが気付かれずに潜伏していた状態が数ヶ月続いていたことは衝撃的と言えます。

- スマホ・タブレットにおいても、PCと同様にアンチウイルスソフトを導入することが今後重要となります。