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。

●マルウェアが使用する8つの典型的な侵入経路

https://news.mynavi.jp/techplus/article/20221010-2473430/
https://www.esecurityplanet.com/networks/how-you-get-malware/

このニュースをザックリ言うと・・・

- 10月4日(現地時間)、セキュリティニュースサイト「eSecurity Planet」において、「How You Get Malware: 8 Ways Malware Creeps Onto Your Device(マルウェアがあなたのデバイスに侵入する8つの経路)」と題した記事が発表されています。

- 挙げられている侵入経路は「マルバタイジング(不正な広告)」「スピアフィッシング(特定のターゲットに対するフィッシング攻撃)」「Chromeの拡張機能、WordPressのプラグイン等に仕込まれたトロイのダウンロード」「PDFファイルやOfficeファイル」「偽のWebサイト」「不正なモバイルアプリ」「リモートデスクトッププロトコル(RDP)」「(USB等の)リムーバブルハードウェア」となっています。

- また、マルウェアの高度化が進む一方、感染経路は一定のままで、大多数が「Webとメール」からの侵入に集約されるとしています。

- アンチウイルスのパターンファイルにおいて何百万ものマルウェアの異種全てに対するシグネチャを作成することは実質不可能であり、一方で攻撃者やマルウェアがターゲットのPCやシステムに侵入するための経路はほんの一握りであるため、セキュリティソリューションではそちらに集中する必要があるとしています。

AUS便りからの所感等

- 8つの侵入経路は、いずれも10～20年近く前から攻撃者に用いられているものです。

- ブラウザーの拡張やモバイルアプリ等については、当初はマルウェアを含まない安全なものだったのが、アップデートの際にトロイの木馬等が仕込まれるようになったというケースも多く知られています(攻撃者が既存の拡張・アプリを買収して悪用することも珍しくありません)。

- 殆どの侵入経路は攻撃者が直接かつ能動的にマルウェアを感染させるというより、ターゲットがまんまと感染しに来るのを待ち受ける受動的な攻撃と言え、各ユーザーにおいてはOSやブラウザー等を最新に保ち、必ずアンチウイルスソフトを有効にすること、モバイルアプリのインストールは必要最低限とし、不審なものでないかネット上での評判・報告を確認すること、さらに企業・組織においてもUTM等各種ソリューションの導入により、ユーザーが不審なファイルを持ち込んだり、万が一に感染したマルウェアがLAN内外へ拡散したりするのを遮断するよう防御策をとることが肝要です。

TECH+ Powered by マイナビニュース

どのマルウェアも最初の侵入経路は同じ、押さえておくべき侵入経路8選

2022/10/10 18:06　著者：後藤大地

eSecurity Planetはこのほど、「How You Get Malware: 8 Ways Malware Creeps Onto Your Device」が、マルウェアに使用されている8つの典型的な侵入方法を紹介した。

サイバー犯罪者は、機密データや金銭の窃取、ハードウェアやファイルの破壊、ネットワークやデータベースの乗っ取りなど行うためにマルウェアを使用している。

● ECサイトの個人情報漏洩増加、脆弱性の管理を…JIPDECが注意喚起

https://scan.netsecurity.ne.jp/article/2022/10/14/48336.html
https://privacymark.jp/news/system/2022/1012.html

このニュースをザックリ言うと･･･

- 10月12日(日本時間)、日本情報経済社会推進協会(JIPDEC)より、ECサイトからの、クレジットカード情報等個人情報漏洩の恐れに対する注意喚起が出されています。

- 注意喚起では、近年ECサイトの規模に限らず、広範囲で脆弱性を狙った不正アクセス等による漏洩事故が増加しているとしています。

- 全般的な注意点としての6項目の他、サイトの構築・運用保守等を外部に委託している場合について、委託側・受託側それぞれに対する注意点も挙げられています。

AUS便りからの所感

- 全般的な注意点6項目としては「どのようなソフトウェアで構築されているか」の把握」「OSやソフトウェア等の定期的な脆弱性情報の確認、セキュリティパッチ適用等に関する体制の構築・運用」「OSやソフトウェア等を最新のバージョンへアップデート」「不正アクセス等へのリスク対策の実施(不正アクセス検知の仕組み導入、脆弱性診断の実施等)」「従業者へのセキュリティ教育の徹底」および「緊急性の高い脆弱性や不正アクセスを検知した際の対応手順や体制を構築し、従業者へ周知すること」が、構築・運用等の委託側には「ソフトウェア等の必要な知識を有し、自社と同等の実施体制を構築できる委託先を選定する」こと、受託側には「委託元に対して必要な情報（パッチ適用の必要性の提案等含む）を提供する」ことが挙げられています。

- サーバー上で保持していたクレジットカード情報が奪取される事故の多発に対し、決済代行会社を利用し、自社にクレジットカード情報を保持しない仕組みが推奨されたことで、攻撃の手口の方も決済フォームを改ざんするものが主流となりましたが、いずれにおいてもECサイトを構築するフレームワーク等の脆弱性を突くことが主要な攻撃手段であり、WAF(Webアプリケーションファイアウォール)による有害なアクセスの遮断のみに依存せず、根本的な対策として各種ソフトウェアを最新のバージョンに保つことを忘れずに行うべきです。


ScanNetSecurity by iid

脆弱性と脅威／脅威動向

2022.10.14 Fri 8:00

JIPDECが個人情報漏えいの注意喚起、ECサイトの脆弱性管理等を呼びかけ

一般財団法人日本情報経済社会推進協会（JIPDEC）は10月12日、ECサイトにおける個人情報の漏えいについて注意喚起を発表した。JIPDECによると近年、ECサイトの規模に限らず、広範囲で脆弱性を狙った不正アクセス等による漏えい事故が増加しているという。

JIPDECでは、ECサイトの構築・運用の注意点として下記を挙げている。

1.全般的な注意点
・どのようなソフトウェアで構築されているかの把握
・OSやソフトウェア等の定期的な脆弱性情報の確認、セキュリティパッチ適用等に関する体制の構築・運用
・OSやソフトウェア等のバージョン管理（最新バージョンへのアップデート）
・不正アクセス等へのリスク対策の実施
・従業者へのセキュリティ教育の徹底
・緊急性の高い脆弱性や不正アクセスを検知した際の対応手順や体制を構築し、従業者へ周知すること

●パスワードの使い回しがなくならない事情…Malwarebytesが解説

https://news.mynavi.jp/techplus/article/20221004-2470434/
https://www.malwarebytes.com/blog/news/2022/10/why-almost-everything-we-told-you-about-passwords-was-wrong

このニュースをザックリ言うと･･･

- 10月2日(現地時間)、セキュリティベンダーのMalwarebytes社より、ユーザーがパスワードの使い回しを続ける理由についての解説記事が発表されています。

- パスワード管理ツールを開発している複数のベンダーによれば、ユーザーが覚えなければならないパスワードの数は平均100個に上り、今後もさらに増加するとされています。

- 記事では、ユーザーが本当にそれら全てを記憶することは不可能であることから、自分が覚えやすい程度に弱いパスワードを用意し、これを書き留めて再利用している、等の傾向を分析しています。

AUS便りからの所感

TECHI Powered by マイナビニュース

- あるサービスで流出や不正ログインの対象となったアカウントのリストを別のサービスでの不正ログインに使用する、いわゆる「リスト型攻撃」への対策として、推測されにくく、各サービスで異なるパスワードを設定するよう長年呼び掛けられており、併せて複雑なパスワードを生成して保存するようなパスワード管理ツールの利用も推奨されてきました。

- PCへのログイン等、パスワード管理ツールが使用できない(また指紋認証を含めた生体認証等も利用できない)場面では依然紙に印刷あるいは書き留めたパスワードを参照して入力する必要があり、そうした場面でユーザー自身が考えられるパスワードはやはり複雑なものとはなりにくいと思われます。

- 記事では、ユーザーがパスワードとその保存場所、使用頻度について心配することなく、セキュリティに大きな変化をもたらすことができるものとして多要素認証(MFA)を挙げていますが、あらゆるユーザーが多要素認証に慣れ、これを受け入れられるようになるにはさらに時間がかかると予想されます。


ユーザーはなぜパスワードの再利用をやめないのか？

2022/10/04 16:15

著者：後藤大地

Malwarebytesは10月2日(米国時間)、「Why (almost) everything we told you about passwords was wrong」において、パスワードの再利用が止まない理由に、パスワード管理に対するセキュリティ専門家の誤診があると伝えた。Malwarebytesのセキュリティ専門家がパスワードの使い回しを止めるようどんなに助言したとしても実現しない理由が説明されている。

ユーザーに対してアカウントごとに固有パスワードを使用するよう勧めることは、セキュリティ専門家の仕事とされている。パスワードの再利用は、サイバー犯罪者が盗んだパスワードのリストを悪用して他のWebサイトに侵入するクレデンシャルスタッフィング攻撃につながる危険性があるためだ。しかしながら、ユーザーにパスワードの再利用をやめるように促しても、うまくいっていない現状がある。その理由は、セキュリティ専門家がこの問題を誤診してきたからと、Malwarebytesは結論づけている。