— AUS（アルテミス・ユーザ・サポート）便り 2019/01/28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。

●7億7300万件のアカウント情報流出か…平文パスワードも出回る

http://www.itmedia.co.jp/news/articles/1901/18/news077.html

このニュースをザックリ言うと･･･

- 1月17日（現地時間）、セキュリティ研究者のトロイ・ハント氏より、多数のWebサイトから流出した大量のアカウント情報（メールアドレス・パスワード）がハッキングフォーラムに掲載されていると発表されました。

- 発表によれば、アカウント情報はオンラインストレージサービス「MEGA」に12,000本以上のファイル（計87GB超）としてアップロードされ、重複や無関係のデータを含めると11億6000万件以上に上っており、ハッシュ化されていたパスワードが平文に戻されていたケースもあったとされています。

- ハント氏は入力したメールアドレスのアカウントが流出しているかどうかを確認できるサービス「Have I Been Pwned（HIBP）」(※参照)を運営しており、流出データから重複等を除き整理したメールアドレス約7億7300万件およびパスワード約2122万件を反映したとのことです。

- また、流出が確認されたパスワードは決して使用せず、パスワードの使い回しを避ける等の自衛策を講じるよう注意を呼び掛けています。

AUS便りからの所感等

- 流出したアカウント情報をもとに様々なサービスへの不正ログインを試みる、いわゆる「リスト型攻撃」の脅威により、パスワードの設定については、かつて安全とされてきた「定期的な変更」が危険とされ、「使い回しをしないこと」の他、「今回のように流出が発覚した場合は速やかに変更する」ことが重要とされています。

- 前述のとおりHIBPには入力したパスワードが流出していないか確認するサービスもあり、パスワードそのものを外部に送信しない形で確認ができる模様です。

- ともあれ、自分が利用している全てのアカウントの棚卸しを行い、「被害を受けた可能性があるアカウントがないか」のみならず「放置しているアカウントがないか」等をも確認し、適切に管理することが重要です。

ITmedia NEWS

文春オンライン　（※参照）http://bunshun.jp/articles/-/8908

●「インターネットの安全・安心ハンドブック」最新版、NISCが無料公開

https://internet.watch.impress.co.jp/docs/news/1165158.html

このニュースをザックリ言うと・・・

- 1月18日（日本時間）、内閣サイバーセキュリティセンター（NISC）より、サイバーセキュリティの重要性を周知するための「インターネットの安全・安心ハンドブック Ver4.00」が公開されました。

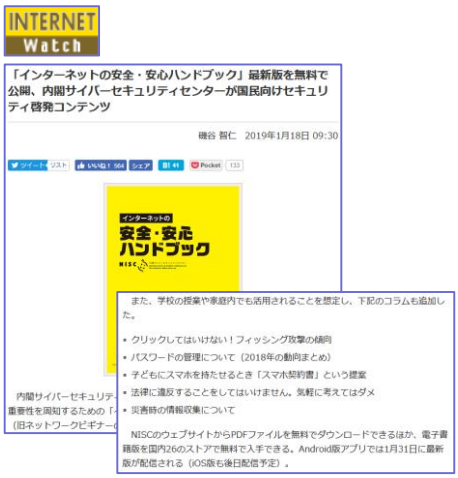
- 2016年2月に「ネットワークビギナーのための情報セキュリティハンドブック」として公開されたもので、ほぼ毎年、最新のサイバー攻撃の事例を反映して改訂されています。

- NISCのWebサイトからPDFファイルが無料でダウンロードでき、各種電子書籍サイトからも同じく無料で入手可能になっています。

AUS便りからの所感等

- 同ハンドブックでは「サイバー攻撃ってなに？」から始まり、
「基本的なセキュリティのポイント」
「最新の攻撃の手口(PC等を乗っ取られることで起こり得ること等)」
「パスワード・Wi-Fi・Web・メールのセキュリティ」
「スマホ・パソコンのより進んだ使い方」
あるいは「SNS・インターネット関連の犯罪やトラブル」まで
広く取り上げられています。

- あらゆる情報機器のユーザはもちろん、システム管理者等においても、利用者に対する教育の題材として、またシステム・ネットワークの見直しやセキュリティソリューションの導入の際にも、「有用な視点」の一つとして活用できることでしょう。



●指令の送受信にGoogleドライブを用いるトロイの木馬を確認

https://japan.zdnet.com/article/35131576/

このニュースをザックリ言うと・・・

- 1月16日（現地時間）から18日にかけて、中国360 Threat Intelligence Center（360TIC）および米Palo Alto Networks社より、「Googleドライブ」を経由して指令のやり取りを行うトロイの木馬の活動について報告されています。

- 報告によれば、トロイは主に中東をターゲットとする攻撃者グループ「DarkHydrus」によるもので、不正なVBAマクロが埋め込まれたExcelファイルの形をとっています。

- 指令のやり取りや、感染したPC上で収集した情報の送信する等の際、特殊なDNSリクエストを用いた通信の他、その代替としてGoogleドライブ上のファイルを用いる機能を持つとされています。

AUS便りからの所感等

- マルウェアが外部からの指令を受ける通信手段も様々で、GoogleドライブのようにHTTPSによる暗号化通信が行われるものもあり、特定のプロトコルを監視するというだけでは完全に防ぎきれないでしょう。

- 外に出ていくあらゆる不審な通信を検知し、時には遮断するような出口対策の採用により、マルウェアの行動を止めたり、機密情報の流出を抑止したりすることが期待できますが、今回のようなことがあったからと、安易にGoogleドライブ等へのアクセスをブロックすることはユーザの利便性を大きく損ねることに注意が必要です。