— AUS（アルテミス・ユーザ・サポート）便り 2017/12/18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。

●ネットバンク狙うマルウェア「DreamBot」、10月以降国内の感染被害急増

http://www.npa.go.jp/cyber/policy/20171211.html
https://www.is702.jp/news/2250/
https://www.jc3.or.jp/topics/dreambot.html

このニュースをザックリ言うと・・・

- 12月11日（日本時間）、警察庁および日本サイバー犯罪対策センター（JC3）より、インターネットバンキングを狙うマルウェア「DreamBot(別名URSNIF, gozi)」への国内の感染被害が10月以降急増しているとして、注意喚起が出されています。

- 警察庁の発表では、DreamBotにより奪取されたアカウント等の件数について、7月～9月は月20件程度であったところ、10月以降は月70件程度に増加しているとしています。

- また、JC3からのウイルスメールへの注意喚起件数も、これまでは月20件前後であったところ、10月に25件、11月には38件と過去最高を記録しています。

AUS便りからの所感等

- 12月におけるJC3からの注意喚起件数は15日の時点で19件にのぼっており、最終的には11月と同程度あるいはそれ以上になると予想されます。

- 先週の当AUS便り（2017/12/11号）で挙げているとおり、国内で確認されているマルウェア拡散メールは他にもいくつかのパターンがありますので、随時情報を確認のうえ、PCへの最新のセキュリティパッチ適用と、アンチウイルス・UTMによる防御を確実に行うようにしてください。

CYBERCRIME PROJECT 警察庁 サイバー犯罪対策プロジェクト

広報・施策

インターネットバンキングに係る
コンピュータウイルスDreamBotに関する注意喚起

平成29年12月11日現在、警察庁では、インターネットバンキングに係るコンピュータウイルスDreamBotに感染したことにより不正に窃取されたインターネットバンキングのユーザID・パスワード等が急増（平成29年７月～９月は月20件程度であったが、10月以降は月70件程度となっている。）していることを確認しています。このことから、DreamBotに感染したパソコンの台数が増加していることが想定されます。

DreamBotは、利用者の入力したユーザID・パスワード等を窃取する機能を有しているほか、遠隔操作を受け不正送金を行う機能などを有しています。

これまでの被害者は、ウイルス対策ソフトを導入していない、ウイルス対策ソフトを導入しているが適切に更新していない状況が見受けられます。ウイルス対策ソフトを導入し、確実に更新を続けることを推奨します。

また、一般財団法人日本サイバー犯罪対策センター(以下「JC3」という)では、DreamBotの感染確認ページを公開していますので、感染の有無を調べるのに活用下さい。

「DreamBot・Gozi感染チェックサイト」
https://www.jc3.or.jp/info/dgcheck.html

また、DreamBotの感染を目的とした不審メールは、実在する組織からのメールを模しているなど、巧妙化しています。コンピュータウイルスの感染を防ぐため、添付ファイルを不用意に開かない、メール本文のリンクを不用意にクリックしないなど、注意して下さい。

TREND MICRO | is702 インターネットセキュリティナレッジ

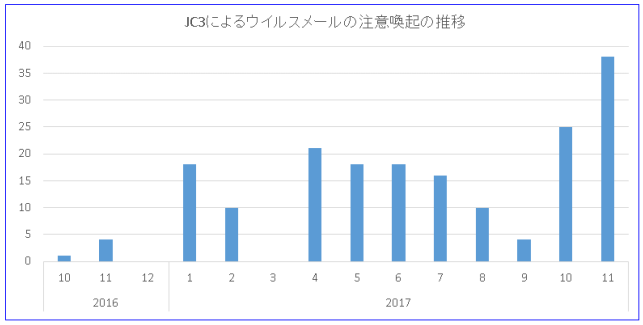
不正送金を行うウイルス「DreamBot」、国内での感染が急増

2017/12/12　ツイート　いいね！5　G+　B!ブックマーク 0　EMail

不正送金を行うウイルス「DreamBot（ドリームボット）」への感染が国内で急増しているとして、警察庁と一般財団法人日本サイバー犯罪対策センター（JC3）は12月11日、注意を呼びかけました。

「DreamBot」は、既存のオンライン銀行詐欺ツールである「URSNIF（アースニフ）」（別名：Gozi(ゴジ)）の不正コードを改造して作成されたと考えられるウイルスです。金融機関のインターネットバンキング用認証情報やクレジットカード情報等を窃取する機能、遠隔操作により不正送金を行う機能を持っています。

JC3 日本サイバー犯罪対策センター



注意喚起件数の推移　（縦軸：件、横軸：年月）

●14億件のアカウント情報が「ダークWeb」に流出…最も多いパスワードは「123456」「123456789」

https://news.mynavi.jp/article/20171215-556255/

このニュースをザックリ言うと・・・

- 12月8日（現地時間）、セキュリティ企業「4iq」の研究者より、ダークWeb（サーチエンジンに表示されない、あるいは特殊な手段でアクセス可能なWebサイト）において、14億件ものアカウントデータを含んだファイルおよびデータベースが確認されたと発表されました。

- 発表によれば、このデータはこれまでに発覚している252件の漏洩事件によるものとされ、ダークWeb上で発見された流出データとしては過去最大のものとされています。

- 流出したアカウントで使われていたパスワードとして最も多いのは「123456」（約920万件）、次いで「123456789」（約310万件）、「qwerty」（約165万件）、「password」（約130万件）となっています。

AUS便りからの所感等

- 今や「数字のみ」「キーボード上の文字を配置順に入力」「単一の英単語」といったパスワードは、攻撃者が様々なパスワードを入力して不正ログインを試みるにあたり、真っ先に狙われるものとなっています。

- 前述したようなものは「最もよく使われるパスワード」として様々な調査で上位に挙がっており（AUS便り 2017/1/23号参照）、Web・メールサービスはもちろん、あらゆる場面で使うべきではありません。

- 今日、パスワード以外にも様々なアカウント保護機構が採用されており、可能な限りそれを利用することも大切ですが、パスワードを狙う攻撃に対しては、例えばツールによる管理を用いてでも、他人から推測されにくい、ある程度複雑なパスワードを設定すること、そして万が一流出が確認され次第、速やかにパスワードの変更を行うことが肝要です。


マイナビニュース

2017/12/15 09:45:43

14億件の平文ログインデータが漏洩、最多のパスワードは?

後藤大地

関連キーワード：情報漏えい

このほど4iQに掲載された記事「1.4 Billion Clear Text Credentials Discovered in a Single Database」が、ダークWebにおいて14億件を超えるアカウントデータを含んだファイルおよびデータベースを発見したと伝えた。

これまでダークWebで発見された流出アカウントデータとしては過去最大規模で、調査の結果、流出したアカウントデータが本物であることも確認されたという。

●ニュースサイトに不正アクセス…改ざん記事、外部サイトにも一時配信される

http://www.itmedia.co.jp/news/articles/1712/14/news063.html

このニュースをザックリ言うと・・・

- 12月13日（日本時間）、ニュースサイト「ナリナリドットコム」より、同サイトが不正アクセスを受け、記事を改ざんされていたと発表されました。

- 発表によれば、不正アクセスは12日20:15頃に発生したとしており、数件の記事が改ざんされましたが、同日中に修復したとのことです。

- この他、同サイトの記事を配信する外部の複数のニュースサイトに、改ざんされた記事が一時配信される事態も発生した模様です。

AUS便りからの所感等

- 今回の改ざんは深刻な害をもたらすものではなかったようですが、そのサイトだけで完結せず、外部のニュースサイトにも少なからず「影響」を与えています。

- また、Webサイトの改ざんが可能であることは、ページ上のコンテンツのみならず、閲覧者に感染するようなマルウェアの挿入や、配布されるツール等の差し替えにも繋がり得ます。

- サーバ上・UTMのような内部から、あるいは外部のサービスからコンテンツの改ざんを監視・検知し、場合によっては修復までを行うような様々なソリューションについて、採用を検討することを推奨致します。


ITmedia NEWS

気になる

2017年12月14日 10時08分 公開

ナリナリドットコムに不正アクセス　記事改ざん被害

「ナリナリドットコム」が不正アクセスを受け、数本の記事が改ざんされていた。

[ITmedia]

118 12 12 17 32

ニュースサイト「ナリナリドットコム」が12月12日夜に不正アクセスを受け、数本の記事が改ざんされていた。運営元のナリナリドットコムは、12日中に記事を修復し、セキュリティを強化したとしている。個人情報は保持していないため、流出の可能性はないという。

同社によると、不正アクセスを受けたのは12日午後8時15分ごろ。不正アクセスの手法や改ざんされた記事の詳細は明らかにしていないが、お笑いコンビ「にゃんこスター」や、「今年の漢字」の記事など3本が改ざんされていたと読者が報告している。改ざんされた記事は、ヤフーが運営するコンテンツサイト「ネタりか」など外部サイトにも配信されていた。

ヤフーは「12日夜に異変に気づき、ネタりかに掲載されていたナリナリドットコムの配信記事を過去の分も含めてすべて12日中に削除した。ナリナリ側の対策を確認した上で、再開する予定だ」としている。