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。

●注文書のPDF、実は偽装したHTML…メールアドレス・パスワード等奪取の恐れ

https://news.mynavi.jp/techplus/article/20260304-4181303/
https://www.malwarebytes.com/blog/threat-intel/2026/03/purchase-order-attachment-isnt-a-pdf-its-phishing-for-your-password
https://www.malwarebytes.com/blog/threat-intel/2025/12/inside-a-purchase-order-pdf-phishing-campaign

このニュースをザックリ言うと･･･

- 3月2日(現地時間)、セキュリティベンダーの米Malwarebytes社より、PDFによる注文書に偽装したファイルでパスワード等を奪取するフィッシング攻撃について注意喚起が出されています。

- 提示されたフィッシングメールの一例では、注文書として「New PO 500PCS.pdf.hTM」というファイルが添付されており、実体は悪意のあるHTMLファイルであるとしています。

- ファイルを開くことにより、偽のパスワード入力フォームが表示され、フォームに入力したパスワード、およびメールが送られたアドレスとユーザーのIPアドレス・位置情報・User-Agent情報等が攻撃者に送信されるとしています。

AUS便りからの所感等

- Malwarebytes社では2025年12月にも注文書に偽装した不審なPDFファイルによるフィッシングの事例を報告しており、PDFファイル上のリンクから外部Webサイト上のフォームに誘導して情報を詐取する手口をとっていました。

- このときは同社製品によってフィッシングサイトへのアクセスがブロックされていた模様で、今回はローカルでHTMLファイルを開かせる手口により、このようなブロックを回避する意図があったものと推測されます(ただし今回も同社製品によって詐欺メールと判定されたとしています)。

- またフィッシングは特定のWebサービスを騙るものではないと思われ、奪取したメールアドレスとパスワードの組み合わせは、「リスト型攻撃」による各サービスへの無差別な不正ログイン等に悪用される恐れがあります。

- 今回のケースのような二重の拡張子を持つ添付ファイル(それ自体はマルウェア感染攻撃等でも使われる古典的な手口で、かつては長大な空白を挟んで本来の拡張子を分かりにくくする等もありました)について特に警戒する他、同社も推奨するようにサービスへの正式なサイトにはブックマークや公式アプリからアクセスすること、アカウントを不正ログインから保護するべく多要素認証を設定すること等が重要です。


TECHF Powered by ASCII
PDF形式の偽の注文書を配布するフィッシング攻撃に注意、アカウント盗まれる恐れ
掲載日 2026/03/04 07:49
著者：後藤大地
Malwarebytesは3月2日(米国時間)、「Purchase order attachment isn't a PDF. It's phishing for your password | Malwarebytes」において、PDF形式の注文書に偽装したHTMLファイルを配布するフィッシング攻撃に注意を喚起した。
このHTMLファイルを開くとパスワードの入力を求められ、パスワードを入力するとネットワーク情報や位置情報などと共に窃取されるという。
Malwarebytes LABS
Personal Business Pricing Partners Resources Help Free Download
SCAMS, THREAT INTEL
Purchase order attachment isn't a PDF. It's phishing for your password
by Pieter Arntz | March 2, 2026
LOGIN
An attachment named New PO 500PCS.pdf.hTM, posing as a purchase order in PDF form, turned out to be something entirely different: a credential-harvesting web page that quietly sent passwords and IP/location data straight to a Telegram bot controlled by an attacker.
Imagine you're in accounts payable, sales, or operations. Your day is a steady flow of invoices, purchase orders, and approvals. An email like this may look like just another item in your daily queue.
Related articles
Purchase order attachment isn't a PDF. It's phishing for your password | Malwarebytes

●uBlock Originの非公式サイトで無関係のサービスが宣伝

https://www.reddit.com/r/uBlockOrigin/comments/1rjtzgc
https://x.com/Yuki27183/status/2028687857381257474

このニュースをザックリ言うと・・・

- 3月3日(米国時間)、掲示板サイトRedditにおいて、Chromeブラウザー向け拡張機能「uBlock Origin(uBO)」の非公式サイトが、無関係のサービスをあたかもuBOと関係のあるサービスと見せかけて宣伝しているとして注意喚起が出されています。

- 当該サイトは「ublockorigin[.]com」というドメイン名で、検索サイトで「uBlock Origin」と検索するとトップに表示され、Google公式拡張ストア上のuBOのページおよび開発者のページにリンクしていますが、開発者とは別の第三者によるサイトとされています。

- 今回、「ublockdns[.]com」という名前のドメイン名で「Multi-device ad blocker」と称するサービスへのリンクがページに貼られたことにより、当該サイトをファンサイトとして扱うべきかの議論が開発者でなされており、開発者のプロジェクトはhttps://github.com/gorhill/uBlock および https://github.com/uBlockOrigin であり、その他はuBOとは無関係であるとRedditに投稿されています。

AUS便りからの所感

reddit

- 1月にはアーカイブ作成・解凍ソフト「7-Zip」の非公式サイトで一時マルウェアを含む偽インストーラーが配布されていたとする報告がありました(AUS便り 2026/01/23号参照)。

- SSHに対応するターミナルソフト「PuTTY」も公式サイト(https://www.chiark.greenend.org.uk/~sgtatham/putty/)と異なるorgサイトが上位に表示されていますが、2025年7月頃からトップページに無関係の政治的な言論が記載されています。

- 知名度の高いソフトウェアの公式のサイトであると誤解させるようなドメイン名を用いる手口はこのように数多く報告されており、ダウンロードの際は単に検索サイトにソフトウェア名を入力した結果だけで判断せず、SNS等での報告等も基に本物の公式サイトへアクセスすることを心掛けてください。

●「24時間以内にVaultのバックアップを」…LastPassを騙るフィッシングに注意喚起

https://blog.lastpass.com/posts/new-phishing-campaign-targeting-lastpass-customers
https://atmarkit.itmedia.co.jp/ait/articles/2602/17/news063.html
https://rocket-boys.co.jp/security-measures-lab/lastpass-warns-of-new-phishing-emails-targeting-customers-fake-vault-backup-alert/

このニュースをザックリ言うと・・・

LastPass

- 1月20日(米国時間)、パスワード管理サービスLastPassより、同サービスを騙りマスターパスワードを奪取しようとするフィッシングが確認されているとして注意喚起が出されています。

- フィッシングの内容は、同サービスがメンテナンスを実施するため、24時間以内にMy LastPass Vaultのバックアップを行うよう呼び掛けるもので、「mail-lastpass[.]com」といったドメイン名の偽サイト等に誘導してマスターパスワードを入力させるものとみられます(3月6日時点で当該ドメイン名や提示されているフィッシングサイトは凍結されています)。

AUS便りからの所感

- フィッシング攻撃の実施は米国の祝日・連休(1月17日～19日)に重なっており、人員が少ない隙を狙い、検知・対応を遅らせる意図があったとされています。

- LastPassでは、スタッフがユーザーのマスターパスワードを尋ねることは決してないとしています。

- 他のパスワード管理ツールでも同様に、マスターパスワードの奪取は保存されたあらゆるパスワード情報の流出に繋がり得ることから、入力の際は正規のアプリ・サイトであることを十分に確認する必要があり、またそのようなリスクもあって大抵は多要素認証(MFA)を提供していることから、MFAの設定も決して怠ることなく実施するよう心掛けましょう。