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。

●エクスプローラーのアドレスバーから不正なスクリプト入力… 「ClickFix」の亜種「FileFix」に注意喚起

https://forest.watch.impress.co.jp/docs/serial/yajiuma/2062226.html
https://www.kaspersky.com/blog/filefix-attack-windows-file-explorer/54752/
https://expel.com/blog/cache-smuggling-when-a-picture-isnt-a-thousand-words/

このニュースをザックリ言うと･･･

- 11月10日(現地時間)、セキュリティ企業のKaspersky社より、いわゆる「ClickFix」攻撃の亜種が確認されたとして注意喚起が出されています。

- ClickFixでは「Win+R」で表示される「ファイル名を指定して実行」に不正なコマンドを入力させてマルウェアに感染するよう誘導していましたが、「FileFix」と名付けられた今回の亜種ではエクスプローラーのアドレスバーからコマンドを入力させるものとなっています。

- 同社は、ファイルエクスプローラーのウィンドウは馴染みのある要素であり、その使用が危険であると認識しづらく、手口に慣れていないユーザーが罠に陥る可能性が非常に高くなるとしています。

AUS便りからの所感等

- 「ファイル名を指定して実行」から、あるいはコマンドプロンプトからとほぼ同様に、エクスプローラーのアドレスバーからもコマンド入力が可能であり、例えばあるフォルダーを開いている状態で「cmd」と打ち込むことにより、コマンドプロンプトをそのフォルダーにいる状態で開くことが可能といったテクニックが良く紹介されます。

- FileFixはClickFixと同様、非常に長いコマンドをクリップボードにコピーし、アドレスバーに貼り付けさせる手口となりますが、途中に長大な空白を入れる等して、単純なファイルパスを入力させるものと誤認識させようとする模様です。

- 注意喚起では、ClickFixの際に回避策として挙げた、Win+Rによる「ファイル名を指定して実行」のブロックのような手法がとりにくいとし、全ての従業員の業務用デバイスに危険なコードの実行を適時に検出してブロックできるようなソリューションを導入することや、ClickFixないしその亜種が行うようなソーシャルエンジニアリングの手法についての啓発・教育を推奨しています。

Impress Watch

PCを乗っとる「ClickFix」攻撃に早くも亜種、「FileFix」にも注意 ～Kasperskyが解説

［Windows］＋［R］キーを押さなきゃ大丈夫……なんて安心してると騙される

樽井 秀人　2025年11月11日 14:26

最近、『PCのトラブルを解決する！』『サブスクが無料になる裏ワザ』などとユーザーをだまし、［ファイル名を指定して実行］ダイアログ（［Windows］＋［R］キー）から悪意あるコマンドを実行させる「ClickFix」という攻撃が流行の兆しを見せています。

しかし、セキュリティソフトでおなじみのKasperskyによると、これの新しいバージョンがすでに確認されているとのこと。この攻撃は「FileFix」と呼ばれており、基本的には「エクスプローラー」のアドレスバーからコマンドを実行させるのが特徴です。

『え、エクスプローラーのアドレスバーってコマンドを実行できるの？』と思ったあなた！　実はそうなんです。今開いているフォルダーで「コマンド プロンプト」を実行する裏ワザなどが有名ですね。

●新聞社の社内Slackにマルウェア感染で不正アクセス…社員・取引先等17,368人分情報流出

https://www.itmedia.co.jp/news/articles/2511/04/news122.html
https://www.nikkei.com/article/DGXZQOUD28CC40Y5A021C2000000/
https://www.nikkei.co.jp/nikkeiinfo/news/information/1393.html

このニュースをザックリ言うと･･･

－11月4日(日本時間)、日本経済新聞社より、同社が社内で利用していたSlackが不正ログインを受け、社員・取引先等の情報が流出した疑いがあると発表されました。

－発表によれば、Slackに登録されていた氏名・メールアドレス・チャット履歴等17,368人分を閲覧された可能性があるとされています。

－同社社員の個人所有のPCがマルウェアに感染したことにより、Slackの認証情報を奪取され、社員のアカウントに不正ログインされたとのことで、同社では9月に被害を把握し、パスワードを変更する等の対策をとったとしています。

AUS便りからの所感

－Slackでは基本的にパスワードまたはメールで送られるマジックリンクによるログインとなり、加えて2要素認証(2FA)を有効にし、SMSで届くコードかワンタイムパスワード(TOTP)を入力させる設定とすることにより、別途スマートフォンと組み合わせない限りログインは困難となる程度にはアカウントを保護することが可能です。

－一方で今回はいわゆるインフォスティーラー型マルウェアがPC上からログイン済みセッションに関係するCookie情報等を奪取したものと考えられ(そしてマルウェアがスマートフォンの方に侵入しないとも決して限りません)、企業・家庭に拘らずアンチウイルス等による防御策はともかく、このようなケースに対しアカウントの保護、ワークスペースへの侵入の防止を行うためにSlack側でさらなる高度なセキュリティ対策がとられるかにも注目したいところです。

ITmedia NEWS

日本経済新聞社、社内チャット「Slack」に不正ログイン　社員の個人PCのウイルス感染が原因

2025年11月04日 19時09分 公開　［松浦立樹，ITmedia］

日本経済新聞社は11月4日、社内で利用しているチャットツール「Slack」に外部からの不正ログインがあったと発表した。社員の個人PCがウイルスに感染し、Slackの認証情報が流出したのが原因。これにより、社員や取引先などの情報が漏えいした可能性がある。

漏えいした可能性がある情報は、Slackに登録されていた1万7368人分の氏名やメールアドレス、チャット履歴など。取材先や取材に関する情報の漏えいは確認していないという。Slack認証情報の流出被害を確認したのは9月で、被害把握後はパスワード変更などの対応を取った。

● 11月の月例セキュリティアップデート、Microsoft・Zoom等発表

https://forest.watch.impress.co.jp/docs/news/2062496.html
https://msrc.microsoft.com/blog/2025/11/202511-security-update/
https://forest.watch.impress.co.jp/docs/news/2062979.html
https://forest.watch.impress.co.jp/docs/news/2062551.html

このニュースをザックリ言うと･･･

－11月11日(日本時間)、マイクロソフト(以下・MS)より、Windows・Office等同社製品に対する月例のセキュリティアップデートがリリースされています。

－Windowsの最新バージョンはWindows 11 24H2・25H2 KB5068861(ビルド 26100.7171・26200.7171)および11 23H2 KB5068865(ビルド 22631.6199)となり、修正された脆弱点のうちWindowsの1件が既に悪用が確認され、Office・Visual Studio等の脆弱性4件について、危険度が4段階中最高の「Critical」と評価されています。

－またZoom社からはZoomクライアントにリモートから攻撃可能なもの等9件が発表され、8月18日リリースの6.5.10で対策済みとしています(Windows版の最新バージョンは10月27日リリースの6.6.6)。

AUS便りからの所感

－無償サポートが終了したWindows 10 22H2は延長サポート(ESU)登録者向けにKB5068781(ビルド19045.6575)がリリースされています(Windows 11 22H2およびそれ以前はアップデート終了のため、25H2等へのアップグレードが必要です)。

－なお10においてESUの登録に失敗するケースが報告され、KB5068781の直前に定例外パッチとしてKB5071959(ビルド 19045.6466)がリリースされており、登録できない場合はKB5071959にアップデートすることが推奨されています。

－いわゆる「パッチチューズデー(米国時間での第2火曜日にあたる)」におけるMS他の月例のセキュリティアップデートをはじめ、各種ソフトウェアベンダーが定期的(隔月・四半期毎等)に行うアップデートについて、特にシステム管理者においては忘れず意識し、OS・機器のファームウェアから各種アプリケーションに至るまで計画的に更新、加えてアンチウイルス・UTM等による多重防御策により、常に脆弱性への攻撃に備えるよう心掛けてください。

Impress Watch

Microsoft、2025年11月の「Windows Update」を実施 ～Windows 10 ESUに初めてのパッチ

「Windows 11 バージョン 23H2」のHome/Proエディションはサービス終了

樽井 秀人　2025年11月12日 11:05

Microsoft、2025年11月の「Windows Update」「Microsoft Update」を実施

米Microsoftは11月11日（現地時間）、すべてのサポート中バージョンのWindowsに対し、月例のセキュリティ更新プログラムをリリースした（パッチチューズデー）。現在、「Windows Update」や「Windows Update カタログ」などから入手可能。Windows以外の製品も含め、今月のパッチではCVE番号ベースで63件（サードパーティーのものを含めると68件）の脆弱性が新たに対処されている。