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。

● パスワード管理ツール「KeePass」のトロイの木馬バージョンによるパスワード奪取攻撃

https://www.withsecure.com/en/whats-new/pressroom/withsecure-uncovers-trojanised-keepass-campaign-in-ransomware-investigation
https://gbhackers.com/hackers-weaponize-keepass-password-manager-to-spread-malware/
https://cybersecuritynews.com/hackers-weaponize-keepass-password-manager/

このニュースをザックリ言うと･･･

- 5月8日(現地時間)、セキュリティベンダーのWithSecure社より、パスワード管理ツール「KeePass」を狙った攻撃について報告されています。

- 報告によれば、攻撃者はトロイの木馬として動作する不正なKeePassを偽のWebサイトからダウンロード・インストールさせ、KeePassのデータベースに保存されたパスワードだけでなく、ブラウザーに保存された各種認証情報等も奪取するとされています。

- 不正なKeePassは、インストーラーは攻撃者の取得した正規の証明書で署名され、トロイとしての活動以外は本物のKeePassとして動作する等、巧妙な偽装がされていたとのことです。

AUS便りからの所感等

- 単にマルウェアをPCに感染させてデータベースファイルを奪取するのではなく、オープンソースソフトであるKeePassの改造版を用いることにより、それが持つデータベースの読み取り機能を生かしたより効果的なパスワード情報の奪取等を意図しているとみられます。

- パスワード管理ツールの形態は、パスワードをクラウド等に保存するサービスと、ローカルに保存するツールとに大きく分けられますが、PCがマルウェアに感染されたり、あるいは今回のようにツール自体にトロイが含まれるものを実行したりした場合、ツールの形態に拘らず全てのパスワードが流出するリスクがあることに特に注意し、アプリの公式サイトや信頼されたアプリストアからインストールするよう心掛けてください。

Helsinki, Finland – May 12, 2025: WithSecure's Incident Response and Threat Intelligence teams have uncovered a sophisticated cyber attack leveraging a trojanised version of the popular open-source password manager KeePass, during an investigation into a ransomware incident in February 2025.

WithSecure urges organizations to remain vigilant against supply chain compromises, carefully verify downloads, and monitor for unusual behavior around credential stores.

The investigation revealed that attackers modified KeePass source code and signed it with legitimate certificates, creating a trusted but malicious version distributed via search engine malvertising. This altered KeePass installer secretly exfiltrated password database contents, while also acting as a delivery mechanism for post-exploitation tools like Cobalt Strike beacons.

● Steamより過去送信のSMS流出、最大8,900万件も

https://www.itmedia.co.jp/news/articles/2505/15/news143.html
https://www.bleepingcomputer.com/news/security/twilio-denies-breach-following-leak-of-alleged-steam-2fa-codes/
https://store.steampowered.com/news/app/593110?emclan=103582791457287600&emgid=533224478739530145

このニュースをザックリ言うと・・・

- 5月13日(現地時間)、米IT系メディアBleeping Computerより、ゲームプラットフォーム「Steam」のユーザーへ過去に送信されたSMSテキストメッセージが外部に漏洩したと報じられています。
- Steamユーザー記録8,900万件以上を保持していると主張するクラッカーからの投稿を受けてのもので、テキストメッセージには受信者の電話番号とSteamのワンタイムパスコードが記載されていたとしています。
- オンライン電話・SMSサービス「Twilio」が侵害を受けた可能性が指摘されていますが、Twilioはこれを否定しています。
- 同15日にはSteamを運営する米Valve社から声明があり、流出は同社のシステムの侵害によるものでもなく、Steamアカウントが特定できる形での電話番号・パスワード・支払情報等の個人データとは関連付けられていなかったとしています。

AUS便りからの所感

- SMSでのパスコード送信による認証については、SIMスワップと呼ばれる攻撃でユーザーの電話番号を不正に奪取することによりアカウントを乗っ取る手口が指摘されています。
- Steamではスマホアプリと組み合わせてのより安全な多要素認証による保護機構「Steamガードモバイル認証」が提供されており、同様の機構を持つ他のサービスについても、可能な限り設定を行っておくことが推奨されます。

ITmedia NEWS

Steam、過去のSMSメッセージ漏えい　電話番号や当時のワンタイムパスワード記載　8900万件規模との報道も

2025年05月15日 15時09分 公開　[ITmedia]

米Valveは5月15日、PCゲーム配信プラットフォーム「Steam」で情報漏えいがあったと発表した。漏えいした情報は、受信者の電話番号を含む、Steamのワンタイムパスコードが記載された過去のSMSテキストメッセージ。規模は明らかにしていないが、セキュリティ企業の発信や米BleepingComputerの報道によれば、8900万件以上が対象になっている可能性もあるという。BleepingComputerは、Steamが導入する米Twilioのサービスが漏えい経路だった可能性も指摘しているが、Twilioは否定したと報じている。

● Microsoft等月例のセキュリティアップデート、Chromeも週一のアップデート

https://forest.watch.impress.co.jp/docs/news/2013834.html
https://msrc.microsoft.com/blog/2025/05/202505-security-update/
https://forest.watch.impress.co.jp/docs/news/2013833.html
https://forest.watch.impress.co.jp/docs/news/2013517.html
https://forest.watch.impress.co.jp/docs/news/2014230.html

このニュースをザックリ言うと・・・

- 5月14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 10 22H2 KB5058379(ビルド 19045.5854)、11 23H2 KB5058405(ビルド 22631.5335)および11 24H2 KB5058411(ビルド 26100.4061)等となります。
- この他同13日にはApple社からSafari・iOS・iPadOS・macOS等について、14日にはAdobe社よりColdFusion・Illustrator・Photoshop等12製品について、同15日にはGoogle Chromeブラウザーについてそれぞれ、セキュリティアップデートがリリースされています。

AUS便りからの所感

- MSの月例アップデートでは5件の脆弱性が既に悪用を確認、2件が攻撃手法が公知となっている他、Office・リモートデスクトップサービス等11件が特に危険度が高い(4段階中最高の「Critical」)と評価されています。
- Chromeで修正された4件の脆弱性の中には、Webサービスのアカウント乗っ取りに悪用される可能性がセキュリティ研究者によって示されており、最新バージョン(Windows版は136.0.7103.114、Android版は136.0.7103.125)への更新を確実に行うことが推奨されます。
- MSの「パッチチューズデー(米国時間での第2火曜日にあたる)」を中心にソフトウェアベンダー各社が定期的に行うアップデート、またWindows 10(およびOffice 2016・2019)については10月15日の無償サポート終了まで半年を切ったことをそれぞれ意識し、特にシステム管理者においてはOS・ファームウェアないし各種アプリケーションのアップデートやリプレースの計画的な実施、加えてアンチウイルス・UTM等による多重防御の実行を適切に行いましょう。

Impress Watch

攻撃報告のあるゼロデイ脆弱性は5件 ～Microsoft、2025年5月の「Windows Update」を実施

CVE番号ベースで75件にとどまるも、注意を要するものは多め

樽井 秀人　2025年5月14日 09:11

米Microsoftは5月13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75件（サードパーティーのものも含めれば82件）の脆弱性が新たに対処されている。