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-Zipの非公式サイトでバックドア入りインストーラー配布か、IIJが注意喚起

https://wizsafe.iij.ad.jp/2026/01/2075/
https://forest.watch.impress.co.jp/docs/serial/yajiuma/2080170.html

このニュースをザックリ言うと・・・

- 1月22日(日本時間)、IIJ社より、アーカイブ作成・解凍ソフト「7-Zip」の非公式Webサイトの中に偽のインストーラーを配布するものが確認されているとして注意喚起が出されています。

- 当該サイトは「7zip[.]com」というドメイン名で、最新バージョンの「ダウンロード」リンクの一部が別のドメイン名「update.7zip[.]cloud」から偽のインストーラーファイルをダウンロードするものとなっており、これを実行すると正規の7-Zipと共に「C:¥Windows¥SysWOW64¥hero¥hero.exe」として「Helper Service」プログラムがインストールされるとしています。

-当該プログラムはシステム権限で動作し、VPN機能を持つとされ、攻撃者がPCにリモートアクセスしたり、ファイルを攻撃者のインフラにアップロードするなどの行為が想定されるとしています。

- 同社ではサーチエンジンで「7-Zip ダウンロード」等と検索した場合に当該サイトが上位に表示されることを確認しているとし、ダウンロードの際は公式サイト(https://www.7-zip.org/)にアクセスする等を呼び掛けています。

AUS便りからの所感等

- IIJでは当該サイトについて、以前は正式なインストーラーにリンクしていたという情報があったとし、またインターネットアーカイブ(https://web.archive.org/)でも1月19日時点で、リンクが公式サイト上のURLを指していたことが確認されており、状況的にしばらく安全な非公式サイトを装い、悪意を以て不正なリンクの差し替えを行った可能性が考えられます。

- 現在もサーチエンジンで前述した検索を行うと比較的上位に表示されることが確認できる(逆に正規サイトが1ページ目に表示されないケースもあります)一方、注意喚起の記事もヒットするようになっており、このような情報が出回っていることに注意を払い、安易に上位のリンクから偽サイトに誘導されないよう慎重に行動すること、ファイルのダウンロードや実行時にあたってもアンチウイルスやUTMによる防御を行うことが重要です。

- 12月23日には、国産テキストエディター「EmEditor」の公式サイトが不正アクセスを受け、偽のインストーラーをダウンロードするよう仕掛けられていたことが発覚しており(AUS便り 2025/12/25号参照。同サイトは後日再び改ざんされたことにより、追加の対策も発表されています)、ファイルを配布する側がいわゆる「サプライチェーン攻撃」等に対しても各種万全の防御をとり、ユーザーが安心してインストールやアップデートが行える環境を如何に用意できるかについても注目されるところです。

IIJ Internet Initiative Japan

2026.01.22　執筆者：SOCチーム
非公式7-Zip Webサイトにて公開されているインストーラによる不審なファイルの展開

‖ はじめに

7-Zipはオープンソースで開発・公開されているアーカイバソフトウェアです。7-Zipは公式Webサイトの他に、非公式のWebサイトが複数存在しています。その内の1つにおいて、2026年1月より、不審なファイルを展開するインストーラへのリンクが掲載されています。SOCにおいて、複数のお客様にて当該実行ファイルの実行を確認していることから、本稿では速報として、その内容をご説明します。

‖ 非公式なWebサイト

7-Zipの公式Webサイトは https://www.7-zip.org/ です。しかし、検索エンジンで「7-Zip ダウンロード」などと検索すると、非公式のWebサイトが複数見つかります。中には書章で公開されているWebサイトもあるようですが、その内の1つである、7zip[.]comについて、不審なファイルをインストールするものとして7-Zipのフォーラムで取り上げられています。このWebサイトは検索すると上位に表示されることから、注意が必要です。

当該Webサイトからのリンク先は、以前は正式な7-Zipのインストーラであったとの情報があります。本稿執筆時点においても、Windows ARM版・Linux版・macOS版などについては公式Webサイトへのリンクとなっており、同様の形式であったものと推測されます。しかし2026年1月のある時にWindows x64版・x86版のリンクのみダウンロード先がupdate.7zip[.]cloudに変更されており、現在は不審なファイルを端末上に展開するものとなっています。

Impress Watch

やじうまの杜
「7-Zip」を非公式サイトからダウンロードするな！　危険だぞ～IIJが注意喚起
窓の杜ライブラリは安全にご利用いただけます
椿井 秀人　2026年1月23日 11:12

IIJのセキュリティチームによると、非公式に「7-Zip」を配布している特定のWebサイトで不審な動きがあるとのこと。その非公式サイトでは、以前は正規のインストーラーがダウンロードできたそうですが、2026年1月以降、不審なファイルを展開する悪質なものに差し替えられているとのこと。

窓の杜からダウンロード

「7-Zip」の公式サイトのドメインは「7-zip.org」ですが、この怪しい非公式サイトは「7zip.com」となっており（まぎらわしい！）、しかもいくつかのWeb検索エンジンでは検索結果の上位に現れるようです。

● BINDにDoS攻撃の脆弱性、1個のパケットでDNSサービス不正終了の可能性

https://jprs.jp/tech/security/2026-01-22-bind9-vuln-dets.html
https://kb.isc.org/docs/cve-2025-13878

このニュースをザックリ言うと・・・

- 1月22日(日本時間)、DNSサーバー「BIND」に1件の脆弱点(CVE-2025-13878)が発見されたとして、修正バージョン(9.20.18, 9.18.44)がリリースされました。

- 脆弱点は権威DNSサーバー・キャッシュDNSサーバーのいずれで稼働している場合も影響し、不正な問合せパケット1個の送信により、サーバー上のBINDプロセスを不正終了させ、DoS攻撃を行うことが可能とされています。

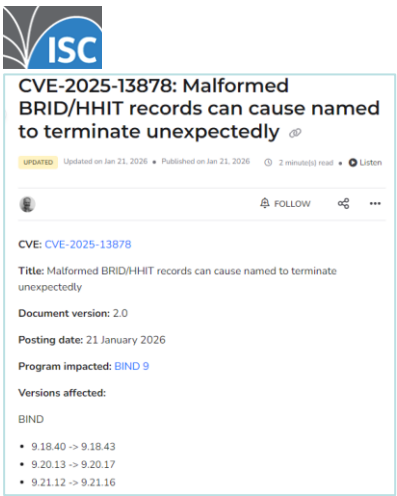
- 同日にはJPRSからも、速やかにアップデートするよう注意喚起が出ています。

AUS便りからの所感

- BINDは最も有名なDNSサーバーソフトウェアとされる一方、長年の間多くの脆弱性が報告されているソフトウェアでもあり、近年は殆どの脆弱性がサーバープロセスのダウンやパフォーマンス低下といったDoS攻撃に繋がるものとなっています。

- 今回の脆弱点は、BIND 9.18系・9.20系の比較的新しいバージョンでのみ影響するとみられ、主なLinuxディストリビューション(安定版)のうちDebianはセキュリティアップデートがリリースされていますが、Ubuntuは影響なし、RHELおよびその派生であるRocky Linux・Almalinux等についても同様に影響なしとなっています。

- 代替として他のソフトウェアあるいはCloudflare・Amazon Route 53等のクラウドサービスを使用するケースも多くなっているものの、ActiveDirectoryとの兼ね合い等でBINDを使用しているケース、メーカー製ネットワーク機器にBINDが組み込まれているケース等において影響が予想され、使用しているソフトウェア・機器のファームウェアについて脆弱性の有無やアップデートのリリース状況を随時確認すること、リリースされ次第適用を行うことが肝要です。



●12月度フィッシング報告件数は190,500件、2月度までは20万件以下で推移か

https://www.antiphishing.jp/report/monthly/202512.html

このニュースをザックリ言うと・・・

- 1月21日(日本時間)、フィッシング対策協議会より、12月に寄せられたフィッシング報告状況が発表されました。

- 12月度の報告件数は190,500件で、11月度(https://www.antiphishing.jp/report/monthly/202511.html)の197,228件から6,728件減少しています。

- 悪用されたブランド件数は114件で11月度(106件)から8件増加、割合が多かったトップ2は先月同様Amazon(約12.6%)、Apple(約6.1%)、次いで報告されたJCB、VISA、セゾンカードと合わせて約31.8%、さらに1,000件以上報告された41ブランドまで含めると約94.8%を占めたとのことです。

- フィッシングサイトのURL件数は55,488件で11月度(52,917件)から2,568件増加、使用されるTLD(トップレベルドメイン名)の割合は .cn(約60.2%)、 .com(約24.7%)の2つが先月同様上位、次いで1,000～10,000件の報告があった .cfd(約5.1%)、.top(約4.2%)、.shop(約2.3%)、.info(約1.0%)、.me(約0.7%)、.net(約0.7%)と併せて約98.9%を占めています。

AUS便りからの所感

- 報告件数は11月に続いて19万件台となり、中国において旧正月となる2月まではこの水準が維持されると推測される一方、3月以降に件数が急増し、さらに上の水準で推移する可能性も十分考えられます。

- フィッシングサイトのURLにおいて「sendgrid.net」の悪用や「amazonaws.com」のホスト名をそのまま使用するケースが増加している他、フィッシング以外で取り上げられている、社長名義で不正なLINEグループの作成に誘導する手口(AUS便り 2025/12/25号参照)についても、OutlookやGMailといったフリーのメールサービスからの送信でSPF・DKIM・DMARCによる検知を回避するものとなっており、正規のサービスが、フィッシングの偽装やメーラーでの検知回避に悪用される事例が目立っています。

- このような手口が出回っていること、不審なメール・SMSについてメールアドレス等を確認するとともに、添付ファイルを開いたりURLをクリックしたりしないこと、本物のサービスへのサイトは事前に登録したブラウザーのブックマークやスマホアプリからアクセスすること等を随時啓発していくことが重要です。