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。

●著作権侵害通知を騙るマルウェア拡散メール…IIJが注意喚起

https://www.itmedia.co.jp/news/articles/2510/07/news095.html
https://wizsafe.iij.ad.jp/2025/10/2018/

このニュースをザックリ言うと･･･

- 10月7日(日本時間)、IIJ社より、著作権侵害通知を装った攻撃メールを8月末頃から複数観測しているとして注意喚起が出されています。

- 攻撃メールはフリーメールサービスのアドレスを送信元とし、マスメディアやエンターテインメント企業を騙り、同意なしにコンテンツを使用したとする文面で、関連する資料として提示されたリンクから不審なzipファイルをダウンロードさせるとしています。

- zipファイルにはWordファイルのアイコンで偽装されたexeファイル等が含まれ、実行により「Rhadamanthys Stealer」や「PXA Stealer」といった情報窃取型マルウェアに感染する恐れがあるとされています。

AUS便りからの所感等

- メールのリンクから複数のURL短縮サービスを経由し、オンラインストレージ上からzipファイルをダウンロードさせる攻撃方法、使用されるマルウェアの種類等、共通した手口の事例が、過去にも世界中で報告されていることも取り上げられています。

- zipファイルにはexeファイル以外にも複数のdllファイルやフォルダーが入っています(例えばPXA StealerはPython言語で書かれたもので、そのためのランタイムを含んでいるとのことです)が、隠しファイル属性が設定され、エクスプローラーの設定次第では表示されない場合があるとしています。

- エクスプローラーの表示設定はデフォルトで「隠しファイル」「ファイル名拡張子」が表示されず、前述のような不審なファイルが隠される他、exeファイル等が他の拡張子に偽装された場合にも判別しにくくなる可能性がある(ファイル名に大量の空白を含めることでexe拡張子を隠そうとするケースにも注意が必要です)ため、安全を考慮してこれらを表示するようチェックを入れることを強く推奨致します(なおアーカイバーソフトでzipファイルの中身を表示した場合は設定に拘らず隠しファイルも表示されます)。

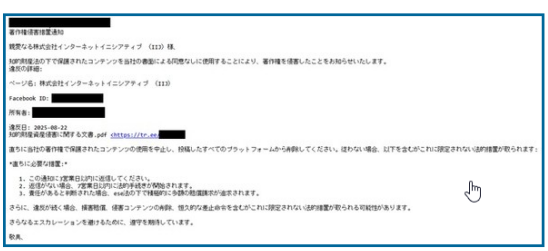
- 上記の設定の他、メールダウンロード時のUTMあるいはPC上でのアンチウイルスによるスキャンも確実に実施するとともに、不審な文面や添付ファイルのメールに対し慎重に対応するよう心掛けることが重要です。

ITmedia NEWS

「あなたのSNS広告で著作権侵害を確認しました、詳細はこちら」→マルウェア配布　IIJが攻撃メールを複数確認

2025年10月07日 16時24分 公開　[ITmedia]

IIJは10月7日、著作権侵害通知をかたり、マルウェアのダウンロードを促すメールを複数確認したとして注意を呼び掛けた。同社の広報問い合わせ窓口でも8月末から複数受信している他、ユーザー企業にも同様のメールが送られているといい、文面などの詳細を公開している。



IIJが確認したメール文面例（同社の報告から引用、以下同）

IIJはフリーメールのアドレスから、マスメディアやエンターテインメント企業をかたって送信するメールを複数確認した。いずれもSNS広告の著作権侵害を指摘する内容で、その資料として短縮したURLを提示する点が特徴。URLにアクセスするとさらに別の短縮URLにリダイレクトされ、ZIPファイルをダウンロードさせられるという。

●韓国政府のデータセンター火災、オンラインストレージ858TB分がバックアップなしで消失

https://gigazine.net/news/20251006-nirs-fire-destroys-government-cloud-storage-no-backups/
https://www.itmedia.co.jp/news/articles/2510/07/news112.html

このニュースをザックリ言うと・・・

- 10月2日(現地時間)、韓国のメディアにおいて、同国の国家情報資源管理院(NIRS)のデータセンターで9月26日に火災が発生し、政府業務用の96の情報システムに被害が出たと報じられています。
- 特に政府職員のデータ保存先に指定されていたオンラインストレージ「G-Drive」については全データ858TB分が消失したとしています。
- G-Driveはバックアップが存在していなかったとのことで、人事管理部署の関係者が「8年分の業務資料が完全に消失した」と話す等の事態となっています。

AUS便りからの所感

- 情報セキュリティ3要素いわゆるCIA(機密性・完全性・可用性)の維持・確保にあたっては、サイバー攻撃等に留まらず、災害等によるシステムの破壊・停止への意識も当然必要となります。
- 10月1日にアサヒビールがランサムウェアによるとみられるサイバー攻撃でシステムがダウンし、依然障害が続いていますが、一方で過去には地方病院がランサムウェア攻撃を受けた際、オフラインに隔離していたバックアップからデータが復旧できたという事例もあります。
- データバックアップを確実に実施することは言うまでもなく、後で確実に復元できることも意識したテストも併せて実施すること、またバックアップ先サーバーの設置あるいはバックアップメディアの保管を物理的に隔離した場所に行うことも、今回のような災害での事例を鑑みるならば欠かせないでしょう。

GIGAZINE

2025年10月06日 13時41分 メモ

韓国の電子行政サービスや政府系クラウドの基盤である国家情報資源管理院で火災が発生しクラウドストレージ「G-Drive」が全焼、バックアップがなく完全に消失してしまうデータも

韓国の国家情報資源管理院(NIRS)のデータセンターで2025年9月26日に発生した火災により、政府の運用するクラウドストレージ「G-Drive」が完全に焼けてしまい、一部のデータが完全に失われてしまったことが明らかになりました。NIRSはG-Driveのほか、ICTインフラや電子行政サービスなどを含む、韓国政府の省庁を横断した国家レベルの統合データセンターで、政府職員のデータ保存先に指定されていました。

新たに、2025年10月1日(水)になって韓国の中央行政機関である**行政安全部**が、NIRSで発生した火災により韓国政府が運用するクラウドストレージシステムである「G-Drive」が全焼し、約75万人の公務員が個別に保存していた業務ファイルが完全に失われたと発表しました。

G-Driveは2018年から運用されており、公務員はすべての業務文書を個人のPCではなくクラウドに保存することを義務付けられ、1人あたり約30GBのクラウドストレージを利用可能となっていました。しかし、義務付けられていたにもかかわらず、実際に使用していたのは政府職員の17%に相当する12万5000人程度で、保存されているデータの総量は858TBだったとのこと。なお、システムは大容量な一方で性能は低く、バックアップは存在していませんでした。

●熊本県警メールサーバー不正アクセス、スパムメール約12万件送信の踏み台に

https://kumanichi.com/articles/1910726
https://www.yomiuri.co.jp/national/20251007-OYT1T50218/

このニュースをザックリ言うと・・・

- 10月7日(日本時間)、熊本県警察本部(以下・県警)より、県警のメールサーバーが海外から不正アクセスを受け、メール不正送信の踏み台にされたと発表されました。
- 業務用メールアカウントに不正ログインされたとみられ、同6日の午前4時45分～午後5時半頃にかけて約12万件のメールが国内外の不特定多数へ送信された(うち約1.9000件が相手に受信された)としています。
- 被害を受けたメールアカウントは既に無効化され、また捜査等に関する資料の管理はインターネットに接続していないシステムで行われているため流出の可能性はないとしている一方、外部に送信されたメールの内容は不明とのことです。

AUS便りからの所感

- メールサーバーへの不正アクセスについては、9月にも中央大学で、サーバーに保存されていたメールの一部情報を読み取られたとする事案が発生しています(AUS便り 2025/10/02号参照)。
- 他者のメールサーバーを迷惑メール等の大量送信に悪用することは、サーバー上の任意のSMTP認証アカウントに不正にログインすることによって可能であり、各メールアカウントにおいて十分強力なパスワードを設定することはセキュリティ面での大前提です。
- かつクライアントPC上に感染したマルウェアからメール送信を行う手口も当然考えられることから、アンチウイルスやUTMによる保護、またメールサーバー側でも不自然な内容・量の外部へのメール送信を遮断するような機構の導入を検討する等が肝要です。

熊本日日新聞

熊本県警サーバーに不正アクセス　外部にメール12万件送信　情報流出やウイルス感染なし

熊本日日新聞　2025年10月7日 21:30

熊本県警は7日、県警のメールサーバーが国外から不正アクセスを受けてアカウントが乗っ取られ、国内外の宛先に約12万件のメールが送信されたと発表した。このうち約1万9千件が到達したが、情報流出やウイルス感染は確認されていないとしている。県警は不正アクセス禁止法違反の疑いで調べる。

情報管理課によると、捜査などに関する重要資料はインターネットに接続していない独自のシステムで管理しており、流出の恐れはないとしている。現時点でメールの到達先から問い合わせはなく、被害も確認されていない。

同課によると、6日午前4時45分～午後5時半ごろ、県警のメールアカウントから大量のメールが送信されていた。複数の海外サーバーを経由して不正アクセスが試みられた可能性があるという。この時間帯に職員から「メールが送信できない」と同課に複数の相談があり発覚した。