— AUS（アルテミス・ユーザ・サポート）便り 2021/08/18号 —
https://www.artemis-jp.com

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。

●製粉業大手、サイバー攻撃でデータ暗号化…復元できず、システム障害も

https://www.itmedia.co.jp/news/articles/2108/17/news121.html
https://www3.nhk.or.jp/news/html/20210805/k10013184001000.html
https://www.nippn.co.jp/topics/index.html

このニュースをザックリ言うと･･･

- 7月9日(日本時間)、国内製粉業大手のニップン社より、同社システムにてマルウェア感染による障害が発生したと発表されました。

- 発表によれば、障害は7月7日早朝に発生し、サーバーの停止、ネットワークの遮断を行って原因調査を行うとしていましたが、8月5日の続報の時点でも、財務・会計等ビジネス活動に必要な基幹アプリケーションの一部が利用できない等、システムの復旧が完了せず、同日予定していた四半期決算発表を延期する等の事態となったとのことです。

- 8月16日に同社より障害の詳細について発表があり、データの暗号化等を行う大規模なサイバー攻撃を受けた可能性が高く、暗号化されたデータの復元やシステムの復旧が行えていない状況であるとしています。

AUS便りからの所感等

- システムにはデータバックアップを行うサーバーも存在していたとのことですが、これも攻撃を受けてデータを暗号化されたとみられることが、データの復元が困難だとしている一因とみられます。

- 現在も度々発生しているランサムウェアによる症状と似通っていますが、発表からはランサムウェアの攻撃を受けたと読み取れる箇所はなく、データ復元のための身代金要求があったかは現在不明です。

- ランサムウェアが最初に流行した頃から言われていたことですが、バックアップデータの保護のため、バックアップデータを保存するサーバーあるいはメディアは常時ネットワークに接続せず、バックアップ実行時以外はオフラインとすること、また単に定期的にバックアップを実行する体制をとるのみならず、確実にバックアップからの復元・システムの復旧を実施できることを確認することが、システムの可用性・完全性他を保持するために肝要となります。

ITmedia NEWS

日本の製粉大手に「前例ない」大規模攻撃　大量データ暗号化　起動不能、バックアップもダメで「復旧困難」

2021年08月17日 16時46分 公開　　[松浦立樹，ITmedia]

印刷　17692　Share　B! 1019

「システムの起動そのものが不可能で、データ復旧の手段はない」――製粉大手のニップン（東証一部上場）は8月16日、7月7日に受けたサイバー攻撃の詳細と影響を明らかにした。

グループ会社を含むサーバの大半が同時攻撃を受け、バックアップを含む大量のデータが暗号化されて復旧不能に。外部専門家に「前例のない規模」と報告を受けたという。

財務システムも被害を受け、早期の復旧が困難なため、8月5日に発表予定だった2021年4～6月期の決算は、約3カ月延期。8月16日が提出期限だった四半期報告書の提出も、11月15日に延期する。

●過去最大、仮想通貨約660億円分が一時流出…のち4割返還

https://japan.zdnet.com/article/35175127/
https://www.itmedia.co.jp/news/articles/2108/12/news117.html
https://gigazine.net/news/20210812-hacker-return-stolen-cryptocurrency/

このニュースをザックリ言うと・・・

- 8月10日(現地時間)、暗号資産(仮想通貨)プラットフォーム「Poly Network」の運営より、同システムが攻撃を受け、暗号資産が外部に送金された可能性があると発表されました。
- 被害額は6億ドル(約660億円)分とされ、2018年にCoincheckから約580億円分が流出した事件を超え、過去最大のものとされています。
- のち、同11日には、流出した分の約4割にあたる約2億6,000万ドル(286億円)分が攻撃者とみられる人物から返還されたとのことです。

AUS便りからの所感

- 一時流出した暗号資産の内訳は「イーサリアム」約300億円分、「バイナンスコイン」約270億円分、「USDコイン」約90億円分および「ポリゴン」約6,300円分とされています。
- 攻撃者はシステムの脆弱性を悪用し、暗号資産を移動する権限を改ざんしたとみられ、また一部を返還した意図については、金銭目的ではなく技術誇示である可能性を指摘する声もあります。
- 流出した暗号資産はまだ全額が返還されていないものの、セキュリティ企業による攻撃者の追跡が行われており、今後全てが取り返されるのか、また今回のケースにおけるPoly Network側の問題や流出経緯および今後の対策について、技術的な詳細が発表されるか等が注目されるところです。

暗号資産660億円流出のPoly Network、ハッカーが300億円近くを返却

Jonathan Greig（ZDNet.com）翻訳校正：編集部　2021-08-12 12:26

シェア 9　ツイート　B! 1　noteで書く　Pocket 4

分散型金融プラットフォームをハッキングし、前代未聞となる額の暗号資産（仮想通貨）を盗み出したハッカーが、その多くを返却したという。被害を受けたPoly Networkは米国時間8月11日、6億ドル（約660億円）を超える暗号資産が盗まれたものの、そのうちの2億6000万ドル（約290億円）が返却されたことを明らかにした。

●8月月例パッチにおけるWindows印刷機能の脆弱性修正は一部のみ、引き続き不要ならば停止を

https://news.mynavi.jp/article/20210814-1945667/
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34481
https://kb.cert.org/vuls/id/131152
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36958

このニュースをザックリ言うと・・・

- 8月11日(日本時間)、マイクロソフト(以下・MS)より、月例のセキュリティパッチ(Windows 10向けパッチKB5005033他)がリリースされ、多数の脆弱性が修正されています。
- 当該パッチでは、Windowsの印刷スプーラー(Print Spooler)で報告された脆弱性(AUS便り 2021/07/20号 参照)のうち「CVE-2021-34481」が修正されたとする一方、この直後に同社より、当該パッチで修正されなかった残る脆弱性「CVE-2021-36958」が存在すると発表されました。
- MSでは引き続き、修正パッチがリリースされるまで、不必要な印刷スプーラーの実行を無効にすることを回避策として推奨しています。

AUS便りからの所感

- 印刷スプーラーについては、6月以降、「PrintNightmare」と名付けられたものも含め脆弱性の報告とパッチのリリースが相次いでおり、今回修正された「CVE-2021-34481」については、当初ローカルからのみ攻撃可能とされていたところ、悪意のある外部のプリンターへの接続によっても攻撃を受ける可能性が指摘されており、一方今回未修正の「CVE-2021-36958」については、最初に注意喚起を出したCERT/CCが「リモートから攻撃可能」、今回注意喚起を出したMSは「ローカルから攻撃可能」と情報が錯綜しています。
- 例えローカルからのみ攻撃可能だったとしても、例えば管理者権限でソフトウェアをインストールしようとする際に悪意を持ったコードが実行され、脆弱性を突かれる恐れも考えられますので、アンチウイルス・UTM等によるインストーラー等のスキャンは確実に実施する必要があります。
- パッチのリリースの有無にかかわらず、「印刷を行う予定のないPC」「プリントサーバーでないWindowsサーバー」「Active Directory環境におけるドメインコントローラ」については、MSの情報に従い、サービス管理画面等から印刷スプーラーサービスを停止・無効化し、脆弱性からの確実な回避を行うことを強く推奨致します。

KB5005033でWindows印刷スプーラ脆弱性を修正しきれず、新たな脆弱性発見

2021/08/14 18:38　著者：後藤大地

Microsoftは2021年8月の累積更新プログラムKB5005033において、印刷スプーラ回りの脆弱性を修正する予定だったが、このアップデートだけでは印刷機能回りの脆弱性をすべて修正することはできなかったようだ。

KB5005033をリリースした後、Microsoftは「CVE-2021-36958」を公開し、印刷スプーラサービスにリモートコード実行の脆弱性が存在すると伝えた。本稿執筆時点で、この脆弱性を修正するパッチや更新プログラムは提供されていない。