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。

●大学の個人情報保存USBメモリー紛失相次ぐ…暗号化されていなかった事例、海外でのPC盗難も

https://www.asahi.com/articles/ASR377J3LR37PISC00K.html
https://scan.netsecurity.ne.jp/article/2023/03/14/49054.html
https://www.j-cast.com/2023/03/08457468.html?p=all

このニュースをザックリ言うと･･･

- 3月6日(日本時間)、金沢大学より、同学職員が個人情報を保存したUSBメモリーを学内で紛失したと発表されました。
- USBメモリーに保存されていたのは、同学卒業生8,910名分の個人情報(住所・氏名・ふりがな)とされています。
- 3月9日には、新潟大学より、同学学生1,128名分および同学の事業への関与者50名分の個人情報を保存したUSBメモリーが2022年4月に紛失していたと発表されました。
- この他、2月から3月にかけて、日本大学・東海大学および成蹊大学の教員が海外でノートPCとUSBメモリーを盗難紛失し、のべ5,500件超の個人情報が被害にあったとみられることが発表されています。

AUS便りからの所感等

- 金沢大学の事案では、USBメモリー暗号化等の対策を行っており、情報流出は確認されていないとのことですが、新潟大学の事案については、情報持ち出し時の承諾手続き、および機密情報や外部記録媒体の暗号化を行うとする機密情報取り扱いのガイドラインに従っていなかったとされています。
- 日本大ほか三大学の盗難事件はいずれも2月6日にパリ近郊の空港で置き引きにあったとの発表があり、同一犯による同じ場所での犯行とみられます。
- 盗難による情報漏洩の可能性を抑止するためには、USBメモリーなどの媒体はもちろん、PC自体でもディスクの抜き取りの可能性を考慮して可能な限り暗号化を行うよう努めるとともに、暗号化やPCへのログイン時のパスワードも十分に強力なものとすること等も考慮すべきでしょう。
- 組織が契約するオンラインストレージサービスにデータを保存して都度参照するアプローチは、PCが盗難にあった場合にサービス側でアカウントロック等を行うことでそれ以上の情報への不正アクセスを遮断することが期待できますが、より高度な攻撃による不正ログインを防ぐため、パスワードによる認証のみならず、スマートフォン等と組み合わせた多要素認証も設定することが重要です。

朝日新聞 DIGITAL

卒業生8910人の個人情報入りUSB紛失　金沢大、被害確認されず

朝倉義統　2023年3月8日 10時48分

【石川】金沢大学（は6日、卒業生8910人分の住所と名前、ふりがなの個人情報が入ったUSBメモリーを職員が紛失したと、ホームページで発表した。今のところ個人情報の流出や不正利用などの被害は確認されていないという。

同大の累計の学部卒業生は約9万7千人（2020年度まで）。大学は、USBに個人情報が含まれていた卒業生らに郵便で紛失を通知した。ただ、USBの内容は暗号化され、個人情報を見るには複数のパスワードが必要なように対策がしてある。

ScanNetSecurity by iid

インシデント・事故／インシデント・情報漏えい

2023.3.14 Tue 8:05

新潟大学でUSBメモリを紛失、許可者の承諾を得ず暗号化も行われず

国立大学法人新潟大学は3月9日、個人情報を含むUSBメモリの紛失について発表した。

シェア　ツイート　送る

国立大学法人新潟大学は3月9日、個人情報を含むUSBメモリの紛失について発表した。

これは2022年4月17日に、同学教員が個人情報が保存されたUSBメモリの紛失に気付いたというもので、4月20日に同学に報告を行っている。なお、当該教員が紛失したUSBメモリを最後に確認したのは4月14日とのこと。

● Emotetまたも活動再開か…サイズの大きいファイル添付でウイルスチェック回避図る

https://www.jpcert.or.jp/at/2022/at220006.html
https://www.ipa.go.jp/security/announce/20191202.html#L23

このニュースをザックリ言うと・・・

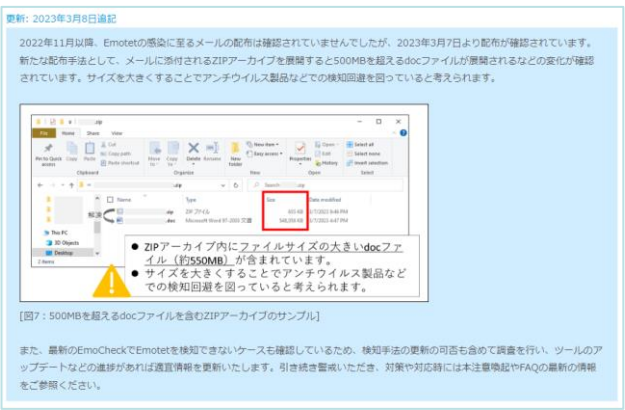
- 3月8日(日本時間)、JPCERT/CC・IPAより、マルウェア「Emotet」の新たな拡散活動が同7日に確認されたとして注意喚起が出されています。
- 各団体によれば、活動が確認されたのは2022年11月上旬以来とのことです。
- 特徴として、約550MBのWordファイル(.doc)を約655KBのzipファイルに圧縮したものがメールに添付されることが挙げられ、これによってアンチウイルスのウイルスチェックを回避する狙いがあると分析されています。

AUS便りからの所感

JPCERT CC Japan Computer Emergency Response Team Coordination Center JPCERT コーディネーションセンター

- JPCERT/CCが提供する検出ツール「Emocheck」の最新バージョン(2022年5月リリース)でも検出できない例があるとされており、同団体によるEmotet注意喚起ページの情報をもとに引き続き警戒を行うよう推奨しています。
- 巨大なファイルに展開されるような不正な圧縮ファイルをマルウェアやその他の攻撃に利用する事例としては、2019年7月に「42KBの圧縮ファイルから計5.5GBの多数のファイルが展開」あるいは「46MBから4.5PBに」といった特殊な圧縮ファイルによる攻撃のコンセプトが発表されており(AUS便り 2019/7/22号)、マルウェアが含まれていなくても、ウイルスチェックを行うUTMやユーザーのPCにおけるメモリ・ディスクリソースの浪費を引き起こされる可能性があります。
- 圧縮ファイルを展開されていない状態で検証し、不審な兆候を検知・遮断できるようにする等、アンチウイルス側での今後の対応に期待したいところです。

マルウェアEmotetの感染再拡大に関する注意喚起



● 「Apache HTTP Server」に2件の脆弱性…2.4.56がリリース

https://forest.watch.impress.co.jp/docs/news/1484555.html
https://scan.netsecurity.ne.jp/article/2023/03/10/49040.html
https://httpd.apache.org/security/vulnerabilities_24.html#2.4.56

このニュースをザックリ言うと・・・

- 3月7日(現地時間)、Webサーバーソフトウェア「Apache HTTP Server(以下・Apache)」の開発元より、Apacheのセキュリティアップデートとなるバージョン2.4.56がリリースされました。
- 修正された脆弱性は、mod_rewrite・mod_proxyのHTTPリクエスト分割の脆弱性(CVE-2023-25690)およびmod_proxy_uwsgiのHTTPレスポンス分割の脆弱性(CVE-2023-27522)の2件とされています。

AUS便りからの所感

Impress Watch

- Apacheでは概ね2～3ヶ月に一度の間隔で不定期にセキュリティアップデートがリリースされています(ただし2.4.54は2022年6月、2.4.55は2023年1月と半年空いています)。
- 脆弱性が発見されたApacheのモジュールのうち、特にmod_rewriteとmod_proxyはリバースプロキシ機能による内部サーバー等との連携で利用頻度が高いとみられ、モジュールを利用していることと、特定の安全でない設定を行っていることが脆弱性を悪用される条件となっています。
- 3月14日現在、Linuxディストリビューションのパッケージではubuntuについてアップデートされていますが、CentOS 7(RHEL 7)・AlmaLinux/Rocky Linux(その他RHEL 8・9ベース)・Debianではまだアップデートはリリースされていません(前述の通り脆弱性の悪用に一定の条件があるためとみられます)ので、リリースが確認され次第、適用を推奨致します。

「Apache HTTP Server」にセキュリティアップデート ～2件の脆弱性を修正

「Apache 2.4.56」への更新を

樽井 秀人　2023年3月9日 12:43

The Apache Software Foundationのリリースページ

The Apache Software Foundationは3月7日、「Apache HTTP Server 2.4.56」を公開した。以下の2件の脆弱性を修正したセキュリティアップデートとなっている。

- **CVE-2023-25690**：mod_rewriteとmod_proxyにおけるHTTPリクエスト分割の問題
- **CVE-2023-27522**：mod_proxy_uwsgiにおけるHTTPレスポンス分割の問題