サイバーセキュリティの置き薬

2022年
第8号

NASを対象とするランサムウェアに注意！

インターネットに接続されたNAS（ネットワークに接続された記憶装置）に対して、保存されているデータやシステム情報を暗号化し使用不能にするランサムウェア「DEADBOLT」（デッドボルト）による被害が確認されています。

本年5月中旬には、新型の「DEADBOLT」が出現し、国内においても中小企業を中心に、業務上必要なデータが使用不能になるなど、事業に大きな打撃を与える被害が発生しています。

「DEADBOLT」の特徴

「DEADBOLT」は、NASを標的とするランサムウェアで、NASの脆弱性を突いて攻撃してくるため、インターネットに接続しているだけで感染し、台湾のQNAP社等が提供するNASで被害が確認されています。

感染すると、NASのデータが暗号化され、ファイルの拡張子が「.deadbolt」に書き換えられたうえ、ログイン画面が乗っ取られます。

さらに、NASの利用者に対し、ファイルを元に戻したければ仮想通貨で身代金を払うよう要求されます。

被害に遭わないよう今すぐ対策を！

- ○ メーカーが提供するアップデートを適用する。
  QNAP社の製品の場合、ソフトウェアをアップデートする必要があります。
  QNAP社のホームページをご確認ください。
  https://www.qnap.com/en-us/security-news/2022/take-immediate-actions-to-secure-qnap-nas-and-update-qts-to-the-latest-available-version
- ○ ソフトウェアのアップデートを行っていないNASは、インターネットから直接アクセスできないようにする。
- ○ 定期的にNASのバックアップを行い、バックアップはネットワークから切り離して保管する。

NASを対象とするランサムウェアは「DEADBOLT」以外にも複数存在します。
ランサムウェア被害を受けた際は、警察への通報をお願いします！