滋賀県警察サイバーセキュリティ情報
R４年度 No. 6
サイバーコネクトSHIG@
今、注目のサイバーセキュリティに関する情報をお届けします。

「DEADBOLT」ランサムウェアに御注意ください！

台湾のストレージメーカーQNAP社製のNAS（ネットワークに接続された記憶装置）に保存されているデータやシステム情報を暗号化して使用不能にする「DEADBOLT」（デッドボルト）と称するランサムウェアによる被害が全国的に発生しています。

「DEADBOLT」によるサイバー攻撃は、本年１月頃から発生していましたが、本年５月13日以降、新型が登場し世界で被害が広がっています。

QNAP社製のNASをお使いの事業者様は、ファームウェアのアップデートを御検討ください。また、QNAP社は他メーカーにNASをOEM供給しており、QNAP社以外の製品が該当する可能性がありますので、重要データをNASに保存されている場合は、使用されている製品の製造元に御確認の上、対応を御検討ください。

「DEADBOLT」による暗号化画像
（引用元：マクニカセキュリティ研究センター
https://security.macnica.co.jp/blog/2022）

～ 被害事例 ～

○ Ａ県内所在の製造業（社員数18人）では、発注書データなどがランサムウェアの被害に遭った。
○ Ｂ県内所在の建設業（社員数６人）では、設計図などのデータが暗号化され、業務に支障が出た。
○ Ｃ県内所在の個人事務所（社員数６人）では、経理データや顧客データなどが暗号化された。

攻撃の概要

「DEADBOLT」ランサムウェアに感染すると、ファイル等が暗号化され、拡張子が「.deadbolt」に変更されます。また、身代金を要求する脅迫文は、テキストファイルとしてNAS内に残されるのではなく、NASへのログインページを改ざんする形で示されます。

「DEADBOLT」による攻撃手法の詳細は明らかになっていませんが、QNAP社の注意喚起情報によると、TS-x51及びTS-x53シリーズの特定のファームウェアのバージョンに存在する脆弱性が狙われている模様です。

措置

QNAP社が提供するファームウェアの最新バージョンへのアップデートを御検討ください。
（参照先 https://www.qnap.com/en-us/security-news/2022/）

アップデートがすぐに実行できない場合は、NASがインターネットに公開されているか確認し、公開されている場合は、ルーターの管理画面から ①ルーターのポートフォワーディング機能を無効にする。 ②QNAPNASのUPnP機能を無効にする。といった一時的な措置を御検討ください。

措置については、IT関連業務を委託されている業者様に御相談していただくほか、QNAP社の注意喚起情報（上記URLを参照）を御確認ください。

被害が発生したり前兆事案を把握された場合は、該当システムを管理する担当者に連絡するほか、警察にも御一報ください。