SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

NAS を標的とするランサムウェア攻撃のハニーポットと動的解析による分析

Analyzing Ransomware Attacks Targeting NAS using Honeypot and Sandbox

安井 浩基 † 井上 貴弘 † 佐々木 貴之 ††
田辺 瑠偉 †† 吉岡 克成 ††, ††† 松本 勉 ††, †††

Yasui Hiroki Inoue Takahiro Sasaki Takayuki
Tanabe Rui Yoshioka Katsunari Matsumoto Tsutomu

キーワード ランサムウェア，ハニーポット，動的解析

あらまし

個人の利用する IoT 機器の一種に NAS（Network Attached Storage）がある．NAS はネットワークを通じて利用できるストレージ機器であり，ユーザは自身のファイルを NAS へ格納することによって，記憶領域の拡張やバックアップの作成などを行う．近年，NAS を標的としたランサムウェアの被害報告が増えている一方で，その攻撃の実態は十分な調査がなされていない．本研究では，NAS を狙うランサムウェアについて，ハニーポットによる攻撃の観測およびマルウェア検体の解析を通して実態の調査を行った．

ハニーポットおよび検体の動的解析には，実際にランサムウェアの被害報告がなされている NAS である QNAP の実機を用いた．ハニーポットとして攻撃を待ち受ける QNAP と検体を動作させて挙動をみる QNAP の二つを用意し，それらを観測用のサーバ機器と接続してネットワークを構成した．観測用のサーバに二つのグローバル IP アドレスを割り振り，ハニーポットの QNAP へ届く攻撃の観測，および動的解析によって検体の発する通信の観測を行った．

ハニーポットでは３か月ほどグローバル IP アドレスを外部へ晒し，QNAP に対してセッションを張る通信を一日あたり平均 130 件ほど観測した．ランサムウェアの感染に繋がる攻撃で，かつ実際に被害報告がでているような既知の攻撃の観測には至らなかったが，アプリケーションのダウンロードや API を用いたシステム操作など，NAS 特有の攻撃を複数回観測することができた．

検体の動的解析では，マルウェアを解析するオンラインサービスである VirusTotal を用い，NAS を狙ったランサムウェアを調査した．そのうち，QNAP の実機で動作する検体については観測用のサーバの下で動的解析を行い，検体の各種挙動を調査した．VirusTotal における検体の調査，および検体の実機解析を行った結果，検体が直接パケットを飛ばすサーバが時期により変化していることや，それらのサーバへ通信を許可しても暗号化挙動に至らないランサムウェア検体のうち，別のサーバへ通信を繋げることで暗号化挙動を観測できるものが存在することなどが判明した．

† 横浜国立大学，〒240-8501 神奈川県横浜市保土ヶ谷区常盤台 79-1, Yokohama National University, 〒240-8501 79-1 Tokiwadai, Hodogaya-ku, Yokohama, Kanagawa, Japan
†† 横浜国立大学先端科学高等研究院，〒240-8501 神奈川県横浜市保土ヶ谷区常盤台 79-5, Yokohama National University Institute of Advanced Sciences, 〒240-8501 79-5 Tokiwadai, Hodogaya-ku, Yokohama, Kanagawa, Japan
††† 横浜国立大学大学院環境情報研究院，〒240-8501 神奈川県横浜市保土ヶ谷区常盤台 79-7, Graduate School of Environment and Information Sciences Yokohama National University, 〒240-8501 79-7 Tokiwadai, Hodogaya-ku, Yokohama, Kanagawa, Japan