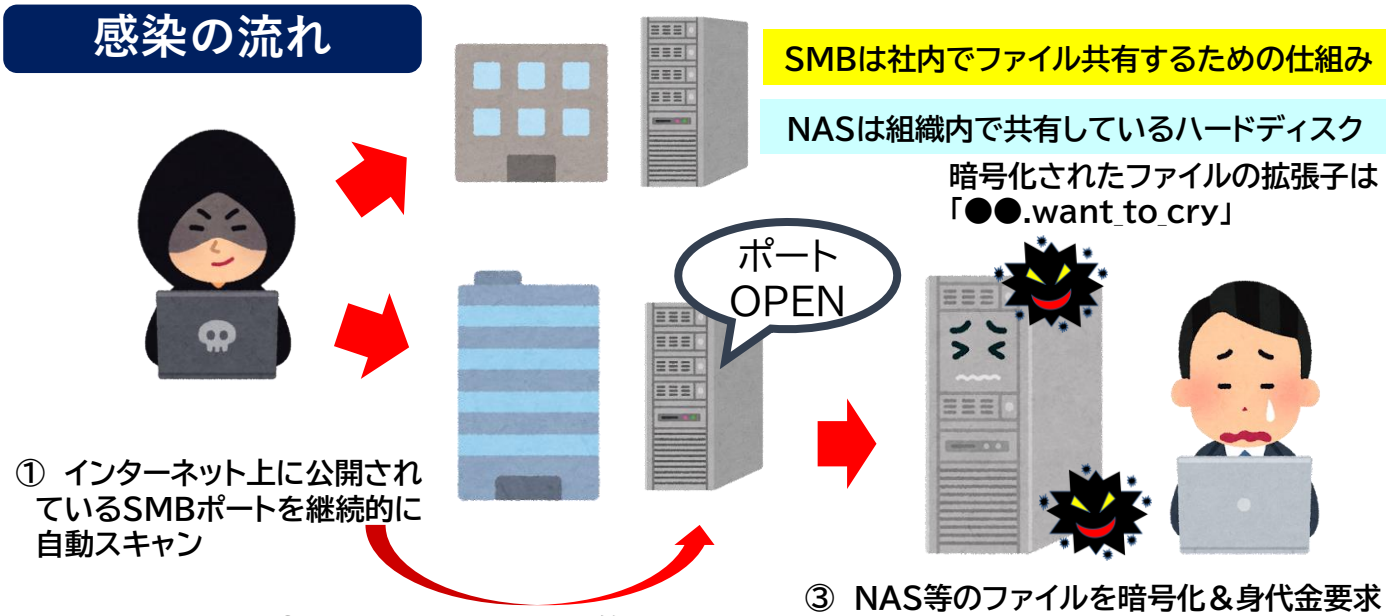
令和 8年8月6日発行

静岡県警察からのお知らせ

「WantToCry」というランサムウェアの被害が増えています

感染の流れ



特徴

① セキュリティソフトが検知しにくい
　マルウェア本体がなく、不正プログラムが実行されないため
② 一般的なランサムウェアとは暗号化の手法が異なる
　攻撃者は遠隔操作でNAS等のファイルを自分の手元に持ち出し、暗号化してから端末に書き戻す
③ 身代金として要求される金額が比較的安い
　一律ではないが数万円から数十万円程度

対策

① 企業内のNAS等がインターネット（外部）に向けてSMBポートの445番、139番（古いポート）を開放していないか確認する、開放していたら閉じる
　※ ルーター、ファイアウォールの設定確認、外部からのポートスキャンも実施
② NAS等への認証は12桁以上の複雑なパスワードを設定する
③ ルータ、NAS等のUPnP機能をオフにする
④ 外出先からNAS等にアクセスする際はVPN機器を介してアクセスする
　（VPNポートを使用すれば445番、139番ポートを閉じることができる）

※ 本資料の内容はインターネット上の情報をもとに作成したものであり、正確性を保証するものではありません。

発行　静岡県警察
　　サイバー対策本部サイバー企画課
TEL　（代表）054－271－0110

静岡県警察サイバー対策本部X
@shizuoka cyber
静岡県警察サイバー対策本部Instagram