サイバー攻撃対策通信

令和７年７月４日
令和７年度第５号
栃木県警察本部
警備部警備第一課

SNSでも情報漏えい対策

2024年５月、北朝鮮を背景とするサイバー攻撃グループ「Trader Trator」（トレイダートレイター）が、国内の暗号資産関連事業者から約482億円相当の暗号資産を窃取しました。

この時に使われた「TraderTrator」の攻撃手法は、ビジネス特化型SNS「LinkedIn」上で、リクルーターになりすまして標的となる会社の従業員に接触し、やり取りを行う中で従業員にマルウェアを業務用PCにダウンロードさせるというものでした。

SNSでやり取りをする相手に悪意があるかどうかを判別することは難しく、被害を防ぐためには予め対策をとっておくことが重要です。

攻撃への対策

もし業務用PCなどがマルウェア感染してしまった際に情報漏えいを防止できるよう、システム管理者として次の対策をとるようにしてください。これらの対策は上記事例に限らず、様々な攻撃に有効です。

システム管理者向け対策
○ 認証ログやアクセスログの取得・監視
○ 必要のないアカウントの削除
○ 各アカウントの権限を必要最小限に設定

また、SNSや端末利用のルールを適切に設定することで、マルウェア感染を防ぐことができます。次の対策を参考としてください。

従業員向け対策
○ 使用を許可されていないPCで業務用システムにアクセスしない
○ SNSでの接触があった場合、相手にビデオ通話を要求する （複数回拒否される場合は不審と判断する）
○ 接触相手のプロフィールやSNS上のやり取りをスクリーンショットで記録しておく
○ プログラムやソースコードの実行を急がせる兆候があった場合は不審と判断する
○ 提供されたソースコードを安易に実行せず、コードの内容を確認する
○ コードを実行する場合は業務用PCを使用しない、または仮想マシンを使用する
○ 不審な接触があった際には上司に相談する