SecDogo Digest 第2号
2026年2月27日 金曜日

特別講演

川崎 真 氏（KELA株式会社 Head of Pre-sales）による「インフォスティーラーによるアカウント侵害の実態とスティーラーログ解析によるサイバー犯罪者の活動の可視化」に関する講演が開催されました。

川崎 真 氏

講演では、ダークウェブインテリジェンスを活用し、インフォスティーラーによるアカウント侵害の現状と、そのログ解析を通じた攻撃者活動の可視化について解説されました。2025年においても感染被害は拡大を続け、総感染端末数は約412万台に達していることが報告されました。スピアフィッシングを起点に、ブラウザに保存された認証情報やカード情報、Cookie、2FA情報、端末情報などが窃取され、闇市場やTelegram上で売買されている実態が紹介されました。特に「Lumma」などのマルウェアの悪用が顕著であることが示されました。

また、生成AI／LLMの活用により、攻撃者が膨大なスティーラーログを自動分析し、効率的に標的選定を行うなど、攻撃の高度化が進んでいる点が強調されました。パスキーやMFAの普及により防御は進展しているものの、盗取済み情報を起点としたリスクは依然として深刻であり、可視化されていない資産の存在が大きな盲点となっていることが指摘されました。

後半では、英国の自動車メーカーJLRへのサイバー攻撃に関与した人物の身元特定事例や、外貨獲得を目的とする北朝鮮IT労働者の活動事例が取り上げられました。スティーラーログ解析を

通じて、日本国内の求人閲覧履歴や翻訳ツール利用痕跡などが確認され、国内企業への関与実態や攻撃者の戦術シフトが明らかになったことが紹介されました。

パネルディスカッション

「今だからこそ問い直すランサムウェア被害からなにを学ぶか～医療×IR×司法で解くランサムウェア対応～」というテーマで、以下のパネリストによるパネルディスカッションが開催されました。

◯ コーディネーター

佐藤 公信 氏（国立研究開発法人情報通信研究機構 サイバーセキュリティネクサス・研究マネージャー）

◯ パネリスト

須藤 泰史 氏（つるぎ町立半田病院）

加藤 智巳 氏（株式会社ラック サイバー・グリッド・ジャパン 主席研究員）

冨士崎 真治 氏（大阪地方検察庁刑事部兼総務部検事 最高検察庁先端犯罪検察ユニット 事務取扱検事）

左から、佐藤 公信 氏、冨士崎 真治 氏、須藤 泰史 氏、加藤 智巳 氏

本パネルディスカッションでは、2021 年のつるぎ町立半田病院のランサムウェア被害を起点に、被害当事者、インシデントレスポンス、司法のそれぞれの視点から、インシデントハンドリングの要点が共有されました。

半田病院の須藤氏は、電子カルテ停止という状況下で患者保護を最優先しつつ、ログ保全の重要性や、経営層が有事の記者会見に備え自組織の状況を正確に把握することの重要性が述べられました。

株式会社ラックの加藤氏は、被害把握と復旧の基盤となるネットワークや PC ログの確保、連絡体制や復旧フローの事前整備が不可欠であると指摘しました。

大阪地方検察庁の冨士崎氏は、犯人特定に必要な情報収集と病院運営への影響抑制の両立が重要であると述べました。

最後に、侵入されることを前提にバックアップデータを守り抜き、システム構成の把握やベンダーとの関係構築、そして平時からのシステム監視が最も重要な行動であると提言されました。