2022 年 3 月 18 日
2022 年 4 月 11 日訂正

各　位

東京コンピュータサービス株式会社

サイバー攻撃による被害と復旧状況について(第三報)

2021 年 12 月 31 日未明に弊社システムがサイバー攻撃を受け、ランサムウェアに感染し、本年 1 月 4 日付け「サイバー攻撃による被害と復旧状況について(第一報)」で公表しました件につき、お客様はじめ関係する皆様に、多大なるご心配をおかけしますことを深くお詫び申し上げます。

第一報でご報告しましたとおり、サイバーセキュリティの専門会社の協力を得て、侵入経路や侵害調査等を進めて参りましたが、その概要が明らかになりました。また、攻撃者が 1 月中旬～下旬、特殊サイト上に窃取したデータを公開したことが明らかになりました。
以下に、これまでに判明した事実について、ご報告いたします。

■第二報以降に判明した事実

(1) 侵入経路・侵害行為について

・攻撃者は、社員向け AD（Active Directory）のパスワードの変更やリセット機能を提供する Web サービスに、リバース Proxy サーバ(*1)を介して侵入接続し、同 Web サービスの脆弱性を利用して AD サーバに侵入したことが、残された痕跡から明らかになりました。

・不正侵入は、2021 年 10 月初旬から発生し、11 月上旬から 12 月末にかけて、侵入行為が行われました。情報の窃取は、この期間に行われたものと考えられますが、窃取された情報の特定は、困難であることがわかりました。

・攻撃者は、上記 Web サービスの脆弱性を利用して、侵入用の実行コードの埋め込みと実行、バックドアの作成、ウイルス対策ソフトウェアを回避するマルウェアの配置を行い、AD ドメインに属する機器に対して、グループポリシー(*2)を利用してランサムウェアを自動的に配布するバッチファイルの配置などを行っていました。

・12 月 31 日早朝、組み込まれたバッチファイルが自動実行され、AD ドメインに属している機器に保存されたファイルの暗号化および拡張子を nightsky に変更する処理を行うプログラムが配布され実行されました。

(*1)　Web サーバへの直接アクセスによる負荷増大やセキュリティリスクを軽減する仕組み

(*2)　ユーザやコンピュータの設定を一元的に管理するための Active Directory の仕組み

(2) 窃取された情報の公開について

これまでの調査で、攻撃者が特殊サイト上に、以下の 2 回、窃取した情報を公開したことが判明しました。

・12 月 31 日早朝から約 1 週間程度【既報】

画像ファイル 6 件（社内管理情報のみ）

・1 月中旬～下旬（公開されていた正確な期間は不明）

ファイルサーバ上に存在していた総量約 5GB のファイル（ファイル数：3242）

1 月中旬～下旬に公開されたファイルの多くは社内管理情報でしたが、一部にお客様やお取引先ご担当者様の情報（会社名、部署名、氏名、等）が記載されたファイルが含まれておりました。その内訳は、以下のとおりです。

・会社名、部署名、氏名、電話番号がわかる情報　［誤］60 件　→［正］58 件

・会社名、部署名、氏名がわかる情報　［誤］26 件　→［正］25 件

（訂正理由：重複が判明した為）

該当するお客様やお取引先様には、個別にご連絡を差し上げ、誠実に対処させていただきます。大変なご心配・ご迷惑をおかけしますこと深くお詫び申し上げます。

■復旧状況

現在、お客様から受注した業務の作業や、お取引先様との連絡業務（メール、オンライン会議、各種情報の処理、等）に利用する PC は、いずれもクリーンインストールを実施し（あるいは新規に購入し）、既存ネットワークとは別に設置したネットワークあるいはモバイルネットワークを利用しております。

また、新たなウイルス対策ソフトウェアを多層に導入し、未知のウイルスを検知する仕組みを強化しております。

全社員に対しては、今回の事象を踏まえて、ランサムウェアに関する情報セキュリティ教育を 1 月に実施しております。

お客様はじめ関係する皆様に多大なるご迷惑をおかけしておりますこと、改めて心からお詫び申し上げます。今後も、窃取された情報の公開を注視して参りますとともに、もし、そのような事象が発見された場合には、漏洩情報の内容に応じて、誠実に対処して参ります。また、再発防止に向けて、サイバーセキュリティの専門会社と協力して、より高いセキュリティ機能を有するシステムの構築や情報セキュリティルールの見直しに全社あげて取り組んで参りますので、何卒よろしくお願い申し上げます。

（お問い合わせ先）
東京コンピュータサービス株式会社 本社機構 業務推進室
03-3815-7911