2017 年 7 月 31 日
株式会社セキュアソフト

注意喚起：スピア型フィッシングによるランサムウェア感染について

1. 概要

ランサムウェア「Wanna Cryptor」や「Erebus」による被害が世界中で報告されておりますが、ランサムウェアの感染原因としてはフィッシング攻撃を利用しランサムウェアへ感染させるといった手法が非常に増えております。フィッシング攻撃は以前より多く報告されており、最近でも大手ソフトウェア会社、大手金融会社等を偽装するフィッシングサイトが多数発見されております。また、JPCERT コーディネーションセンター フィッシング対策協議会からは 2 か月連続でフィッシング報告件数が増加しているとの報告も行われており、より一層の注意が必要です。

（参考情報）

■JPCERT コーディネーションセンター フィッシング対策協議会「フィッシングに関するニュース」
https://www.antiphishing.jp/news/

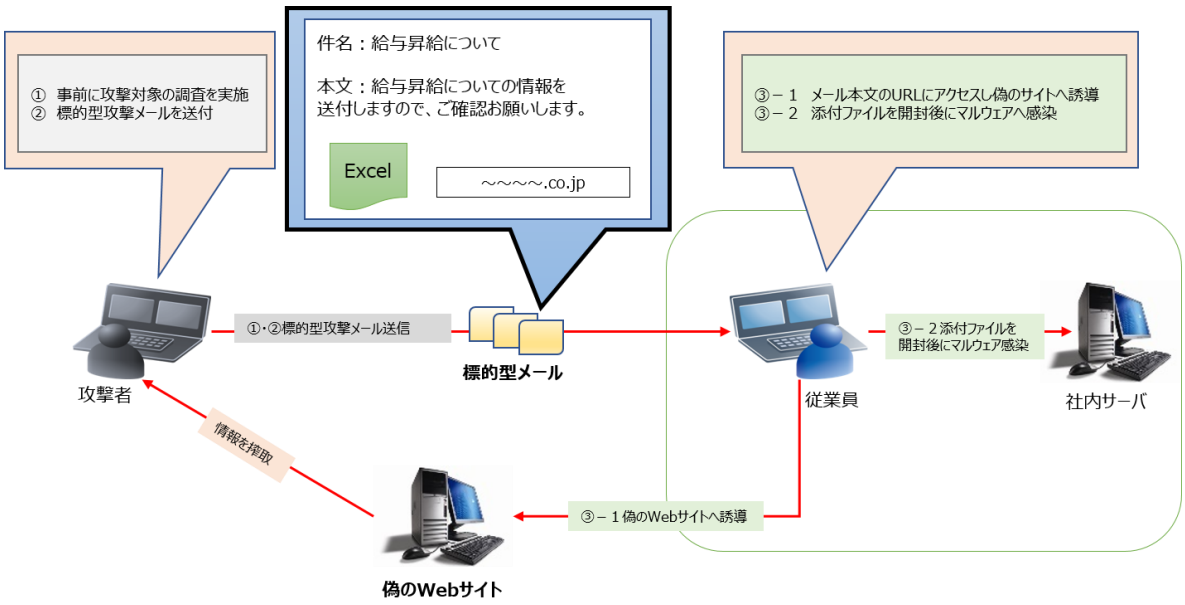
2. スピア型フィッシング攻撃について

⑴ 攻撃の特長

スピア型フィッシング攻撃は標的型攻撃の一種で、その特長は特定の個人や企業/組織等を攻撃対象にしている事です。攻撃者は攻撃対象にソーシャル・エンジニアリングを利用して、個人や組織に関する情報を調査します。その後 E メールでのやりとりを行い、あたかも攻撃対象の知人かのように偽装します。その為攻撃対象が攻撃に気付きにくい点も特長です。攻撃者の目的は攻撃対象が保有する情報や資産を搾取する事です。また、ランサムウェアの配信方法にスピア型フィッシング攻撃を使用するケースが報告されております。メールを受信した攻撃対象がその攻撃に気付く事は非常に困難でその威力は大きく、高い危険度となります。

⑵ 攻撃の手順

① 事前にソーシャル・エンジニアリングを利用して攻撃対象の調査を実施。
② 攻撃対象に関連する情報を利用した巧妙な内容で不審に思われない標的型攻撃メールを送付。
③-1 メール内のリンクから偽サイトへ誘導後情報を搾取
③-2 添付ファイルにランサムウェア等のマルウェアを埋込み開封後に感染



【図　1】スピア型フィッシング攻撃による攻撃イメージ図

⑶ 一般的な対策

① メールの添付ファイルを不用意に開かない。

② 常に個人情報を入力する画面では HTTPS 通信での暗号化通信を使用する。

③ アンチウィルスソフトのアップデートを怠らない。

3. SecureSoft i-コンテナ活用によるスピア型フィッシング攻撃のマルウェア対策

⑴ コンテナ概要説明

SecureSoft i-コンテナは、コンテナ技術を利用したインターネットアクセス専用のネットワーク分離ソリューションです。
上記に記載した対策に加えて、i-コンテナ環境下でのインターネット接続、Web メール使用時にはフィッシング攻撃によるランサムウェアを始めとするマルウェア被害を防止することができます。

⑵ 構成条件と攻撃への対処ロジック

① インターネット接続専用環境側で、メール受信を Web ブラウザメール利用とする。
スピア型フィッシング攻撃メールにより添付されたファイルや URL にアクセスしマルウェアへ感染しても、i-コンテナにより分離されたインターネット接続専用環境だけが攻撃対象となり、通常業務環境に被害が発生しません。
さらに、i-コンテナの仮想ドライブ初期化機能により、マルウェア自体が削除されるため、安全が確保されます。

② 大事な業務データは通常業務環境側での利用・保管・管理とする。
i-コンテナの機能により、通常業務環境側のデータ領域と i-コンテナによるインターネット接続専用環境側のデータ領域は分離されるため、万が一、マルウェアが i-コンテナ内に侵入しても通常業務環境のデータを保護することができます。

【図 2】i-コンテナ環境に侵入したマルウェアの分離イメージ

SecureSoft コンテナ シリーズについての詳しい内容は、下記 URL をご参照ください。
https://www.securesoft.co.jp/products/#container

«お問合せ先»
株式会社セキュアソフト
〒150-0011
東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F
TEL 03-5464-9966
FAX 03-5464-9977
sales@securesoft.co.jp