2020 年 3 月 31 日

サービス＆セキュリティ株式会社 e-Gate センター

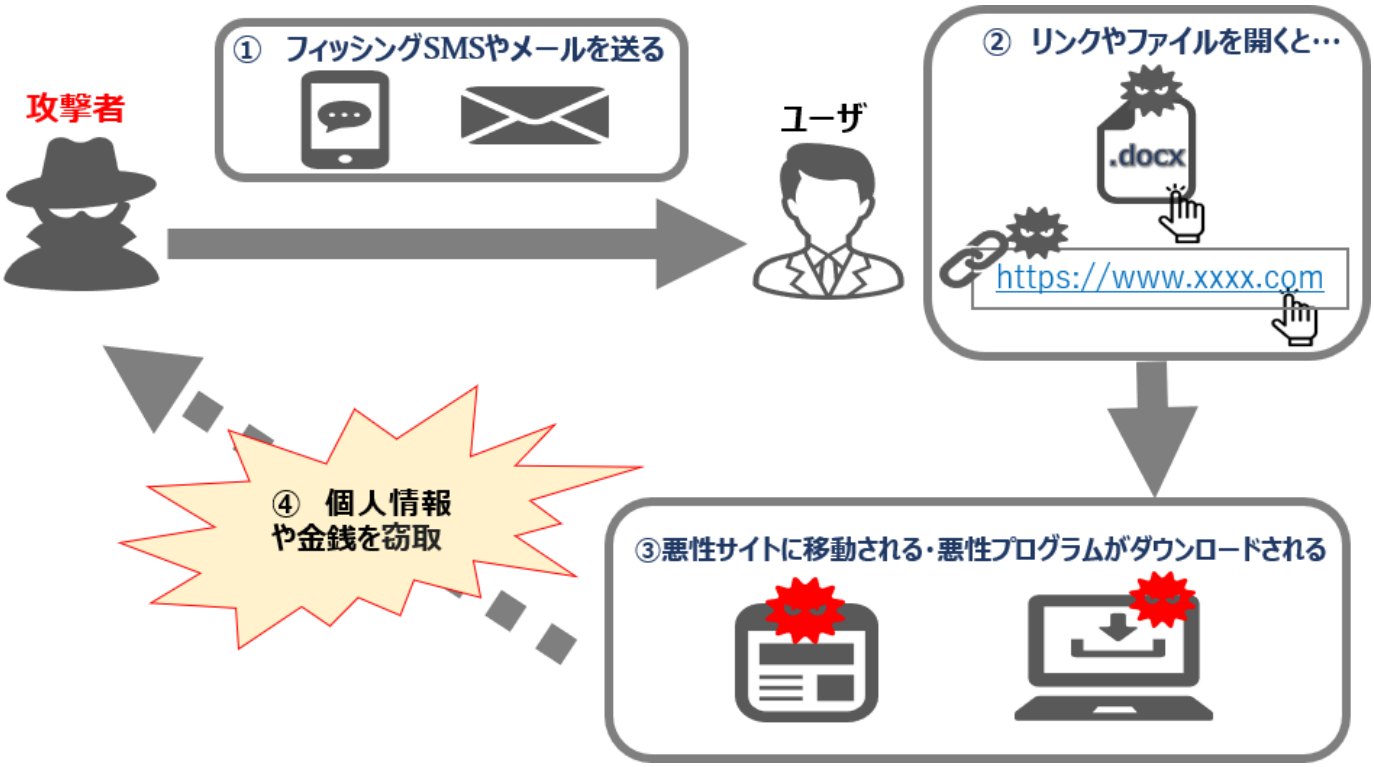
新型コロナウイルスに便乗したフィッシング

1. 概要

新型コロナウイルス(COVID-19)に全世界の注目が集まり、コロナウイルスに便乗したフィッシングが発生しています。新型コロナウイルスは人を介して容易に感染するため、全世界に感染拡大しています。高い感染力と情報不足により、人々に不安と混乱が広がっています。攻撃者は人々の不安や恐怖心につけこみウイルスの予防法・ワクチンなど虚偽の情報を用いて様々なフィッシングをしています。本記事では新型コロナウイルスに便乗した手法と対策についてご紹介いたします。

2. フィッシングの発生について

感染症以外の自然災害やイベントなど全世界の注目が集まった過去の出来事でも、常套手段としてフィッシングが発生しています。



【図１】フィッシングの流れ

フィッシングの手法や特徴について知ることで、フィッシングの被害を防ぐことができます。また、今後発生する社会的トピックに便乗したフィッシングが発生した際にも、攻撃者の攻撃を予測して防ぐことができます。

3. フィッシングの配布方法や攻撃手法について紹介

社会的トピックとイベントに便乗したフィッシングは,メールや SMS を利用し悪質なサイトのリンクや悪性プログラムを配布します。フィッシングの配布方法や手法についてご紹介いたします。

3.1. フィッシング配布方法

SMS とメールはフィッシングの代表的な配布方法です。攻撃者は信頼性の高い機関や企業を騙り SMS やメールを送信します。コロナウイルスに便乗したフィッシングではマスクや感染予防方法などがよく悪用されます。図 2 と 3 は実際に送付された SMS とメールの例です。

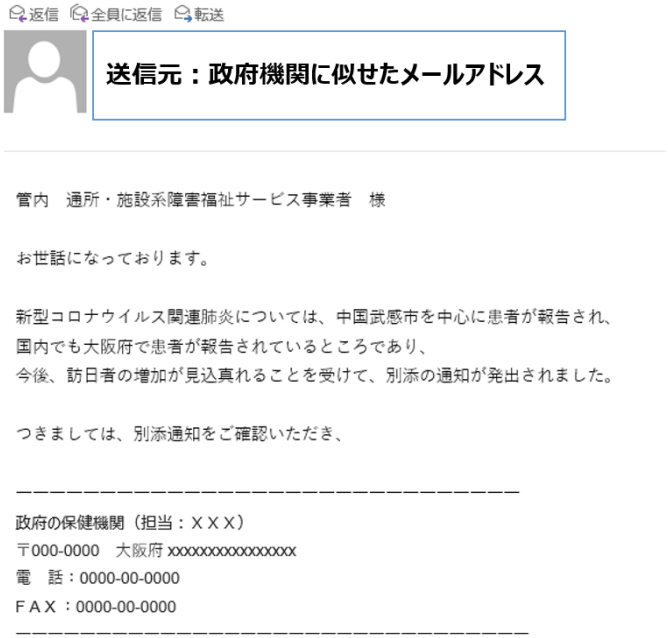
(1) SMS によるフィッシング

図 2 はマスク不足に便乗し、ユーザを悪性サイトに誘導する SMS です。ユーザの心理を悪用したフィッシングの例です。

【図 2】マスクを利用したフィッシングの例

(2) メールによるフィッシング

図 3 は政府機関を騙ったフィッシングです。感染予防方法などを悪用し悪性ファイルを配布します。人々の不安と恐怖心を悪用したフィッシングの例です。



【図 3】政府機関を騙ったフィッシングの例

※ **フィッシングの詳細について以下ニュースを参照ください。**

『フィッシングの最新情報および対策方法』

https://www.ssk-kan.co.jp/topics/topics_cat05/?p=9834

3.2. 悪性サイト攻撃

代表的な悪性サイトは社会的トピックに関連した組織を騙ったフィッシングサイトと偽の製品を販売するフィッシングサイトです。

(1) 社会的トピックに関連した組織を騙ったフィッシングサイト

メールや SMS に記載された URL のリンクをクリックすると、フィッシングサイトに誘導されます。フィッシングサイトは、社会的トピックに関連した機関や企業に似せたサイトで個人情報の入力を要求したり、悪性プログラムをダウンロードさせたりします。

【図 4】フィッシングサイトの例

■ **国際機関や政府機関**

国際機関や政府の保健機関を騙ったウイルスの予防方法などを確認できるフィッシングサイトに誘導されます。フィッシングサイトは本人認証を装い、ユーザに個人情報（ユーザ名とパスワードなど）を要求します。

■ **大手配送業者等**

フィッシングメールに記載されたリンクをクリックすると、大手配送業者にみせかけたフィッシングサイトに誘導されます。フィッシングサイトではマスクを受け取るための個人情報（名前、住所、電話番号など）を要求します。悪性プログラムのダウンロードを要求するサイトもあります。

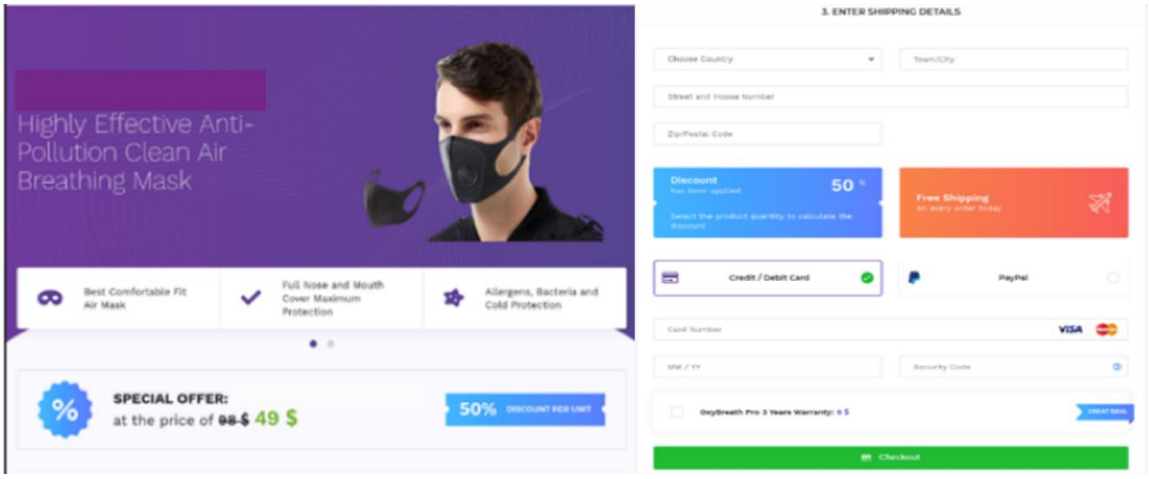
配送業者を騙ったコロナウイルスの影響による配送遅延を知らせるフィッシングメールを送信します。荷物の配送状況を確認するためのページに見せかけたリンクでフィッシングサイトに誘導します。フィッシングサイトは認証ページを装い、ユーザに個人情報（ユーザ名とパスワードなど）を要求します。

(2) 偽の製品販売するフィッシングサイト

社会的トピックに合わせた製品を販売するフィッシングサイトに誘導し、個人情報や金銭を窃取します。

■ **偽のマスク販売サイト**

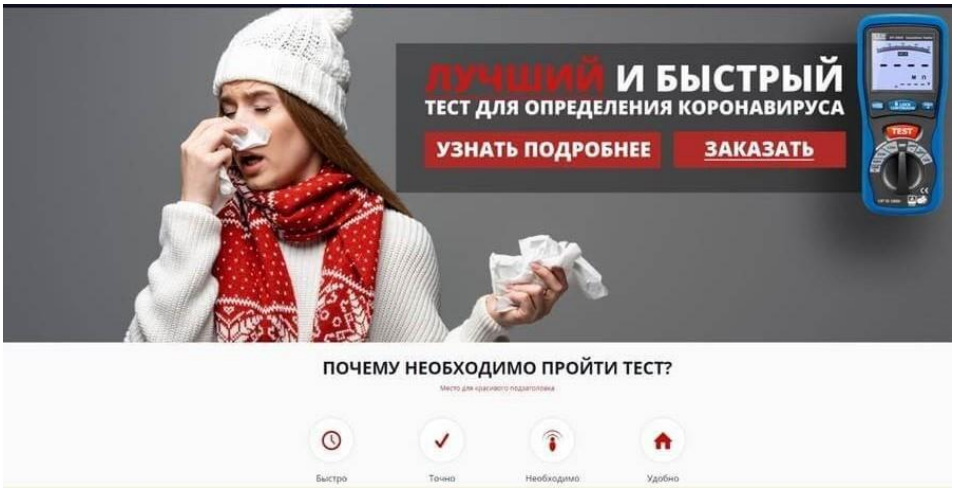
図 5 はマスクを販売しているようにみせかけたフィッシングサイトです。全世界でのマスク不足に便乗したフィッシングで、クレジットカード情報や個人情報（名前、住所、電話番号）などの入力を促し、個人情報や金銭を窃取します。Sky News によると、2 月にイギリスで偽のマスク販売サイトが$ 1,000,000（1 億円）を稼いだといわれています。



【図 5】マスクの販売フィッシングサイト

■ **感染判断機械販売サイト**

図 6 はコロナウイルスの感染判定を謳った機械を販売するサイトです。サイトによると、「自宅で感染判断できる機械を$300（3 万円）にて購入が可能だ」と宣伝しています。しかし、実際にはそのような機械は存在せず、購入することはできません。偽のマスク販売サイトと同様に個人情報や金銭が窃取されてしまいます。



【図 6】偽感染判断機械を販売するフィッシングサイト

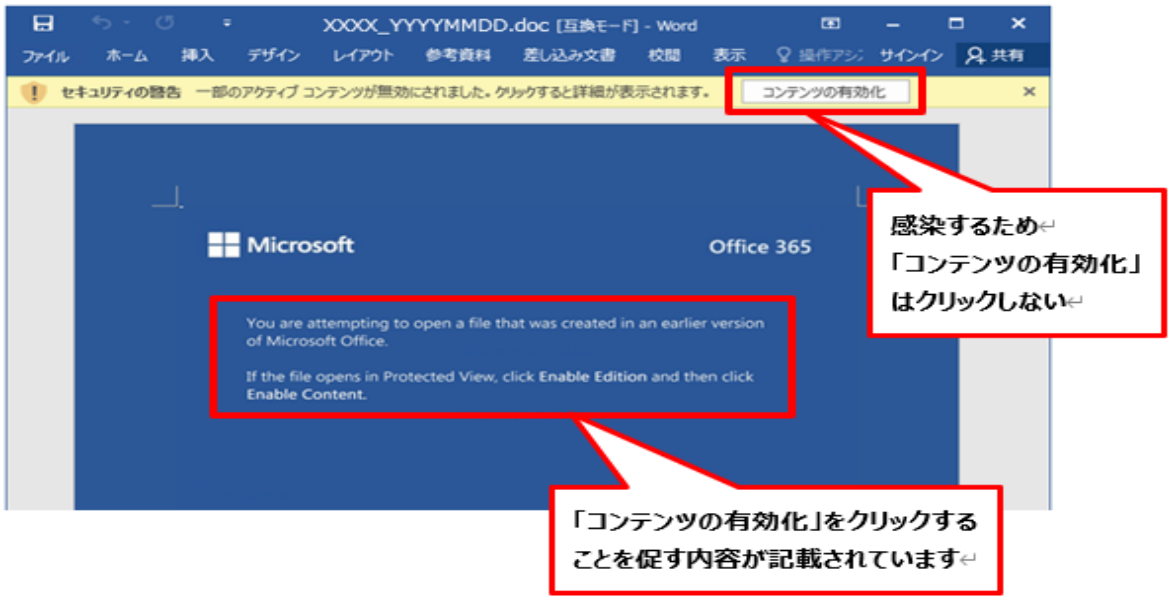
3.3. 悪性プログラム攻撃

悪性プログラムは悪性サイトやメールの添付ファイルを介してダウンロードされます。コロナウイルスに便乗したフィッシングで頻繁に使用される悪性プログラムはマルウェアやランサムウェアなどがあります。この悪性プログラムがダウンロードされると、個人情報と金銭などを窃取します。

(1) Emotet

Emotet は主に Word・PDF などの文書ファイルのマクロを介して感染します。フィッシングメールに添付されたファイルを開くと、Emotet 本体である exe ファイルがダウンロード・実行されます。

下の図 7 はフィッシングメールに添付された Word ファイルの例です。「コンテンツの有効化」ボタンをクリックすると、Emotet 本体である exe ファイルがダウンロード・実行されます。



【図7】Emotetに感染せるWordファイルの例

※「Emotet」の詳細については下記のニュース記事を参照ください。

- **『マルウェア「Emotet」(エモテット)最新攻撃メールについて』**
  https://www.ssk-kan.co.jp/topics/topics_cat05/?p=10400

- **『注意喚起:進化するマルウェア「Emotet」について』**
  https://www.ssk-kan.co.jp/topics/topics_cat05/?p=9657

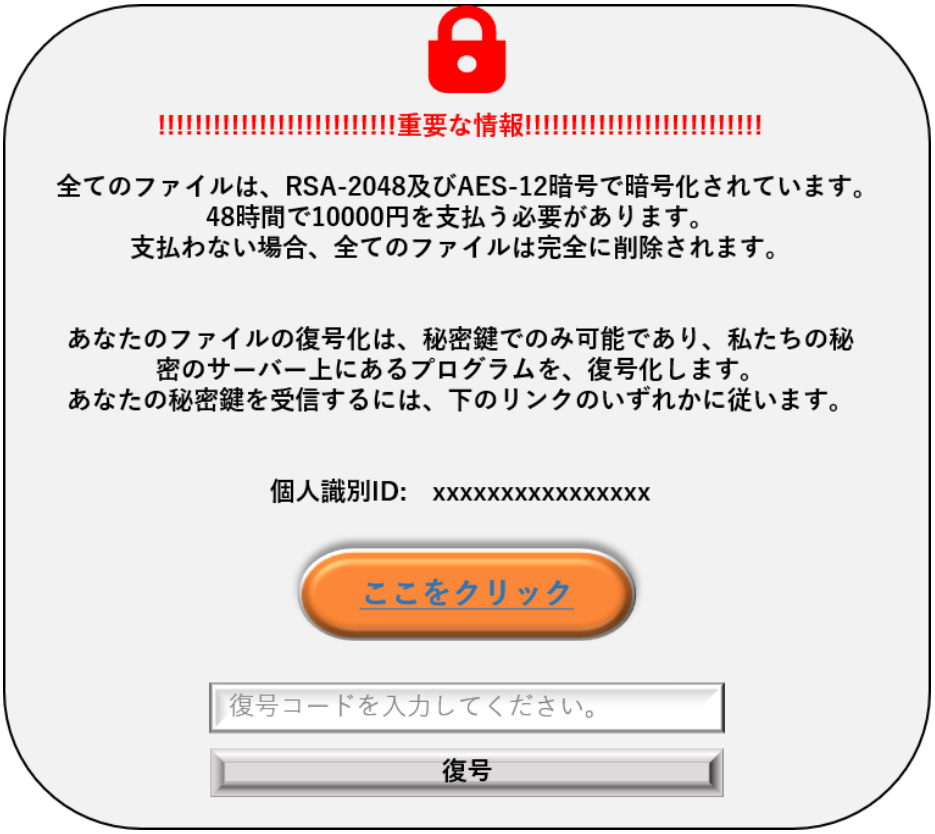
(2) AZORULT マルウェア

AZORULT マルウェアは個人情報などを窃取するマルウェアです。コロナウイルスの感染状況を表示するように見せかけたサイトで配布されていることが確認されています。コロナウイルスの感染状況を確認することができる地図に見せかけ、ファイルをダウンロードさせるように誘導します。ダウンロードしたファイルを実行すると、マルウェアに感染し、ユーザの個人情報を窃取します。

(3) ランサムウェア

ランサムウェアは基本的に不正なメールや悪性サイトを介してダウンロードされます。ランサムウェアに感染すると、ユーザのデバイスとその中にあるファイルを暗号化し図８のような画面が表示されます。暗号化を解除する為の復号化キーを引き換えに金銭を要求します。

CovidLock ランサムウェアという悪性プログラムが急増しています。CovidLock ランサムウェアは悪性サイトの不正なアプリケーションを介してダウンロードさせます。コロナウイルス感染状況を示すサイトを模したフィッシングサイトでは、ユーザにリアルタイムな情報取得の為のアンドロイドアプリケーションのダウンロードを促し、CovidLock ランサムウェアに感染させ、金銭を要求します。



【図 8】ランサムウェアの例

4. フィッシングの対策

3章までで紹介したようなフィッシングに対しては以下の対策がありますので参考にしてください。

- 不審なSMSやメールは開封しない
- メッセージの内容や送信元をよく確認し、メッセージに記載されているURLに安易にアクセスしない
- メールまたは疑わしい Web サイトからプログラムを安易にインストールしない
- 表示されたWebサイトが正しいかどうか、必ずアドレスバーのURLを確認する
  - ドメイン名に不審な点がないか確認する
    - 実際のサイトのドメイン名が“www[.]xxxxx[.]gov[.]jp” の場合、“www[.]xxxxx[.]gov-corona[.]jp”のように偽装していることがある
  - ブラウザのアドレスバーにあるURLがhttps://であることを確認する
    - “http://” は、暗号化がされていないため、個人情報を入力しない
- OS、アプリケーションを最新にする
- アンチウイルスソフトを使用し、パターンファイルを最新にする
- 重要なファイルなどはバックアップし、別のネットワークなどの隔離された場所に保管する
  - 悪性プログラムがファイルを暗号化した場合、バックアップから復元することができる

※ **フィッシングの詳細な対策は以下ニュース記事を参照ください。**

『フィッシングの最新情報および対策方法』

https://www.ssk-kan.co.jp/topics/topics_cat05/?p=9834

5. 参考情報

・IPA 情報処理推進機構

「マルウェア Emotet への対応 FAQ」を更新

https://www.jpcert.or.jp/tips/2020/wr200601.html

・カスペルスキー

【更新】新型コロナウイルス関連情報を装うマルウェアや詐欺メール

https://blog.kaspersky.co.jp/coronavirus-reached-the-web/26781/

・Sky News

Coronavirus: Scammers con face mask buyers out of £800

https://news.sky.com/story/coronavirus-scammers-con-face-mask-buyers-out-of-800k-11953933

・Fox Business

Hackers using coronavirus to scam people, install malware on devices

https://www.foxbusiness.com/technology/hackers-coronavirus-phishing

・Krebs on Security

LIVE CORONAVIRUS MAP USED TO SPREAD MALWARE

https://krebsonsecurity.com/2020/03/live-coronavirus-map-used-to-spread-malware/

・Forbes
Warning: This Malicious Coronavirus Tracker Will Lock Out Your Phone
https://www.forbes.com/sites/zakdoffman/2020/03/16/new-warning-you-must-not-open-this-malicious-coronavirus-app/#1abd51b85763

6. e-Gate の監視サービスについて

今回は主に利用者の方向けのセキュリティ対策についてご紹介させていただきましたが、サービス提供者側のセキュリティ対策も肝要です。安定したサービスの運用には、不正な通信を検知するためのセキュリティ対策の導入と、そのログの監視が重要です。e-Gate のセキュリティ機器運用監視サービスでは、24 時間 365 日、リアルタイムでセキュリティログの有人監視を行っております。サイバー攻撃への対策としてセキュリティ機器を導入する場合、それらの機器の運用監視を行い、通信が攻撃かどうかの分析、判断をして、セキュリティインシデント発生時に適切に対処できるようにすることが重要です。“e-Gate”のセキュリティ監視サービスをご活用頂きますと、迅速なセキュリティインシデント対応が可能となります。

また、e-Gate の脆弱性診断サービスでは、お客様のシステムにて潜在する脆弱性を診断し、診断の結果、検出されたリスクへの対策をご提案させていただいております。

監視サービスや脆弱性診断サービスをご活用いただきますと、セキュリティインシデントの発生を予防、また発生時にも迅速な対処が可能なため、対策コストや被害を抑えることができます。

■総合セキュリティサービス e-Gate

SSK（サービス＆セキュリティ株式会社）が 40 年以上に渡って築き上げてきた IT 運用のノウハウと最新のメソッドで構築した次世代 SOC“e-Gate センター”。この 2 つを融合させることによりお客様の情報セキュリティ全体をトータルにサポートするのが SSK の“e-Gate”サービスです。e-Gate センターを核として人材・運用監視・対策支援という 3 つのサービスを軸に全方位のセキュリティサービスを展開しています。

【参考 URL】
https://www.ssk-kan.co.jp/e-gate/

«お問合せ先»
サービス＆セキュリティ株式会社
〒150-0011
東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F
TEL 03-3499-2077
FAX 03-5464-9977
sales@ssk-kan.co.jp