

アンラボ・セキュリティレター

Press **Ahn**

---

2020.07 Vol.79

半期を掌握したセキュリティ脅威トップ5…新型コロナウイルスの影響大



## 新型コロナウイルスとセキュリティ脅威

# 半期を掌握したセキュリティ脅威トップ5…新型コロナウイルスの影響大

東京オリンピックシーズンを前後に国家的なサイバーセキュリティ脅威が現れると見通しながら出発した2020年。しかし、誰一人として予測できなかった生体ウイルス「新型コロナウイルス感染症（COVID-19、以下「コロナ19」と略）」の登場によって全世界が急激な変化を迎えた。この感染症は私たちの生活のすべてを丸ごと変えてしまったと言っても過言ではない。黄砂とPM2.5の対策用で使用していたマスクが毎日、それも四六時中着用しなければならぬ必需品となった。対外活動時は相手と向かい合っただけの食事や会話を最小化し、社会的距離の確保と生活の中での距離確保を実践しないと健康を保つことができない時代で生きることとなったのだ。遠隔授業や遠隔勤務を通じた非対面、非接触は日常となり、これによる生活の変化は避けられなくなった。社会的距離の確保と生活の中での距離確保の実践が社会のあらゆる面において不便な要素として作用しているが、互いの健康を守るために不便を耐え忍ぶ期間でもあった。私たちの日常が不便になった分、サイバー空間での私たちの生活はどうだったのだろうか。

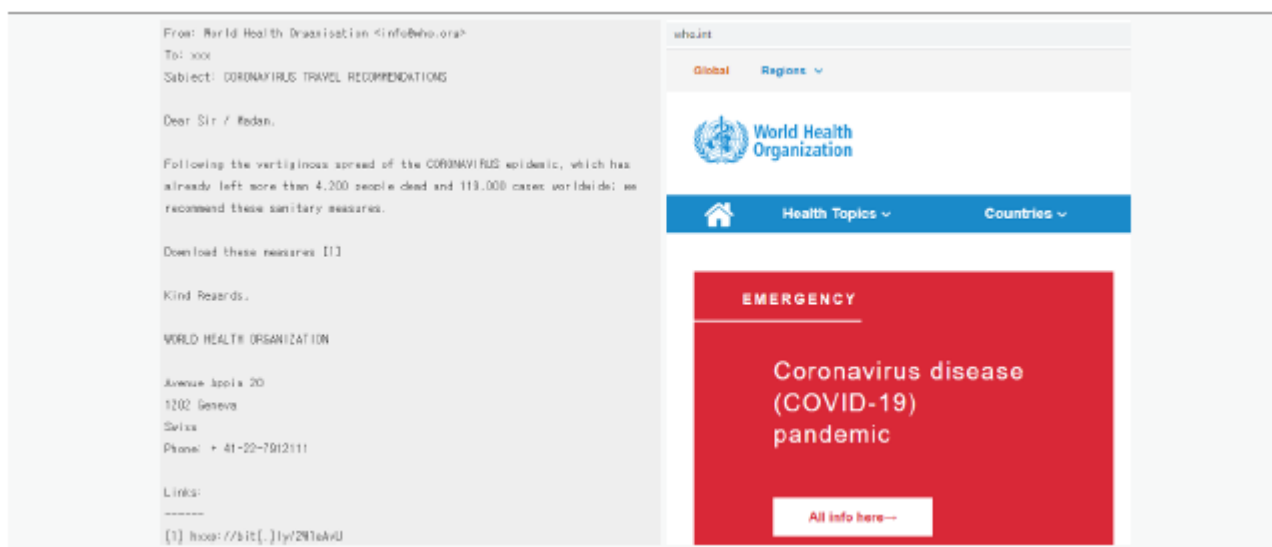
この文ではコロナ19によって急激な変化を迎えた2020年上半期のITセキュリティにおいて、どのような脅威が問題となったのかを調べている。



## 1. コロナ19 情報に偽装したサイバー攻撃

世界保健機関（The World Health Organization、以下「WHO」と略）は2020年3月12日、コロナ19が感染症の警戒レベル、フェーズ6のパンデミック（Pandemic）であることを公式宣言した。さらに、公衆衛生の領域を超えて社会、経済を含むすべての領域に悪影響を及ぼす混乱の時期を、個人と国家がこの脅威に立ち向かって積極的に闘うことを促した。この混乱の時期の隙を狙い、サイバー攻撃の勢力は巧妙に私たちの周りに忍び込んだ。その中の最も代表的なサイバー脅威が、コロナ19情報に偽装したサイバー攻撃である。コロナ19関連情報を含んでいるものと偽装したメールメールウェアは、メール送信者のアドレスを世界保健機関（WHO）、またはアメリカ疾病予防管理センター（CDC）と類似した記録でメール受信者の目を欺いた。

実際、世界保健機関や疾病予防管理センターの正確なURLを認知している人はあまり多くないことから、攻撃者が本物に似せて作り上げたURL及びメールアドレスを見てサイバー攻撃であることを疑ったり、気付いたりすることは殆ど無かったものと推定される。[図1]のWHO偽装メールは送信者のメールアドレスにはwho.orgが使用されたが、実存するWHO公式ホームページのアドレスはwho.intであることが分かる。正常なホームページアドレスが、むしろ非正常的なメールアドレスより偽物のアドレスのような印象を受けたとしても、決しておかしくない程度だ。



[図1] 世界保健機関（WHO）のメールアドレスに偽装したメールとホームページ



【図2】アメリカ疾病予防管理センター（CDC）アドレスに偽装したメールアドレス

## 2. スミッシングとボイスフィッシング

個人の携帯端末であるスマートフォンに対するスミッシング攻撃（Smishing Attack）と、使用者を騙して金銭的な被害を与えるボイスフィッシング攻撃（Voice Phishing Attack）が増加している。正月、お盆、クリスマスなど、知人に挨拶の言葉を送るシーズンや宅配物の溢れかえるようなシーズンが来る頃に行われるものが、メッセージを通して広まるモバイルマルウェアのスミッシングである。

しかし、ライフスタイルの変化によって特殊なシーズンにのみ利用するのではなく、日常でもネット通販サイトを通じた注文が一般化されてきている中、配達状況を知らせてくれる様々なメッセージの受信は日常生活においてかなり自然なことのひとつとなった。特に、コロナ19の影響によってオンライン活動をまともに行うことができず、ネット通販の利用が急増するこの時期を狙ってスマートフォン利用者をターゲットとするスミッシング攻撃が増加した。最も簡単な方法では宅配物の配達案内メッセージに偽装し、利用者の接続を誘導した。過去、スミッシング攻撃グループはスマートフォンのメッセージを短縮URLで構成し、スマートフォン利用者の疑いを最小化した後にURLへの接続を誘導した。メッセージを短縮URLを押すと、攻撃者が事前に作成しておいたAndroidアプリの拡張子であるAPKファイルがダウンロードされる。Androidアプリの公式流通窓口であるGoogle Playストアを通さずに直接悪性APKファイルをインストールするよう誘導していたが、昨年頃から盛んに活動しているスミッシング攻撃グループは、自分たちの攻撃対象者からのアプリダウンロードの試みを区別するためのロジックを追加する緻密さを見せた。自分たちの作った悪性アプリダウンロード用ページをスマートフォンから接続したのか、PCから接続したのか1次的に確認する。

続いて、自分たちが確保したスマートフォンの番号であるかを2次的に検証した後、悪性アプリをダウンロードさせる。これは自分たちが意図しなかった場所に自分たちのアプリが露出されることを最小化するためのものであることが推測される。この過程を通し、悪性アプリのダウンロードURLがマルウェアの分析家やセキュリティ会社に露出されたとしても、攻撃者が作成したフィッシングサイトでなく正常な宅配会社のウェブサイトが開かれ、悪性APKファイルをダウンロードすることができないため、何の妨害も受けずに攻撃をすることができるようになった。このようなスミッシングアプリには、一般的なAndroidアプリに付与される権限より、さらに過度な権限が付与される。これはスミッシングアプリを通し、スマートフォン内部に存在するユーザー情報を収集するという意図を持っていることを表している。

コロナ19状況を効果的に克服するために政府が実施した「政府緊急災難支援金」に関する内容を悪用し、「政府緊急災難支援貸出案内」に藉口したKB国民支援、ウリ金融支援など、制度置銀行の商号の詐称や庶民金融展覧館、国民幸福基金など、公共機関の商品であるかのように詐称し、利用者が公信用のある機関から発送されたメッセージと誤認するよう誘導した。これに加えて「先着順支給」、「限定消費品」などの刺激的な表現で、

緊急資金が必要な人たちの不安な心理を悪用した手口まで確認された。このような被害を受けたくないためにも、メッセージやスマホアプリを利用した悪意ある攻撃についてよく知っておかなければならない。

### 3. 基盤施設ターゲットのサイバー攻撃

サイバー領域で戦略的優位を占めるための努力は絶えず行われている。特に、国家の主要基盤施設のターゲット攻撃を通して基盤施設の内部を掌握し、その後自分たちの目的に合わせて活用する試みが確認された。韓国内の特定団体所属の実際の職員の名前を使用した発信者から関連職責者のみを受信者に制限した後、文書ファイルに偽装したマルウェアが添付されたターゲットメールを送信する、スパイフィッシング攻撃も発見された。

Microsoft Word文書で作成されたこのマルウェアは、内部のマクロファイルを通して悪意的な動作を遂行する。従って、ユーザーが最初に文書を開いた瞬間、セキュリティ警告画面を通して「マクロ実行可否」の選択メニューが表示されるようになっている。該当団体の職員リストを見ると、送信者が実際の勤務者の名前であることが分かった。攻撃者が攻撃に有利な情報を事前に収集し、これを適材適所に活用する緻密さを見せたケースだと言える。メールに添付された文書ファイルを開くと、実際のコロナ19に関する内容が開かれるため、疑わしい部分を発見することは難しいが、該当文書はセキュリティホールを通して攻撃者が意図したマルウェアをインストールするよう作られた状態だった。インストールされたマルウェアの目的によって、該当文書を開いたユーザーのPC内部に保存されている主要情報の収集及び流出するよう動作する。

コロナ19の韓国内での大規模感染者が現れ始めた時期に注目された「新天地」関連資料に偽装した文書ファイルが登場し、ユーザーの文書閲覧を誘導した事例もあった。文書は二種類の内容を含んでおり、ユーザーの疑いを巧妙に避けることができる構造だった。文書を開いた場合、レジストリキーの登録を通してPC再起動後も攻撃者が意図したバックドアが持続的に動作してプロセスリスト、PC名、OSバージョン情報の送信とファイル実行及び終了、追加ファイルダウンロードが行われ、主要情報収集及び流出が可能であることが確認できた。コロナマスク関連の中国内の状況をブリーフィングする内容のターゲットメールが、韓国内の特定企業に流入された事例も確認された。添付された圧縮ファイルを開いて実行すると、PC内の主要情報収集及び流出を遂行する遠隔命令遂行マルウェアである、NanoCore RATがインストール及び動作される。2013年に初めて発見されたNanoCore RATは、PCからデータを収集して攻撃者に伝達するキーロガーのような様々な機能を持っていた。遠隔でPCのオンオフ、ファイルの実行やキーボードの入力値を記録することはもちろん、コンピューターを使用できないようロックし、ウェブカメラを通した録画までも可能としたものが、まさしくNanoCore RATである。前述したターゲット攻撃は、すべて国家主導のサイバー攻撃集団及び彼らと理念を共にする組織によって行われたものであり、特別に韓国内の基幹産業及び防衛産業体をターゲットに行われた攻撃だった。

これらの攻撃グループが狙っているものは、基本的なセキュリティシステムの崩壊を通じた内部アクセスとインフラ掌握及び主要機密情報の収集と流出であり、決定的には「核心技術の流出」と「偵察を通じた対策樹立」を目標としている。私たちがすでに過去の数多くのターゲット攻撃の事例を通して学習しているように、破壊を通じた武器システムの武力化及び社会基盤施設の麻痺は、これらの攻撃者がいつでも選択できるオプションの一つであるだけで、必須項目ではない。韓国内の基幹産業及び防衛産業体をターゲット攻撃するサイバー攻撃グループの攻撃から企業と組織の安全を守るための第一歩は、内部で使用しているメールの添付ファイルに注意することである。これは何処を指しても足りないくらい、最も重要で基本的な部分だ。4～5年前に使用していた韓国産フードプロセッサの攻撃法を再使用していたことが確認されたため、韓国産フードプロセッサの最新バージョンのアップグレードとセキュリティパッチのインストールは必ず行われなければならない。



## 4.OT 環境にまで入り込んだランサムウェア

数多くのITセキュリティ事件や事故の中に埋もれているが、変わらず大きな脅威として位置しているものがランサムウェア（Ransomware）である。その中、産業制御システムをターゲットとしたランサムウェア攻撃に関しても注目する必要がある。2019年3月、ヨーロッパの製造会社をターゲット攻撃してファイルを暗号化し、生産ラインの稼働を止めたLockerGogaは、▲30個の拡張子のみ暗号化 ▲セキュアメール使用 ▲有効なデジタル署名使用 ▲交渉を通して支払額調整 ▲組織の内部情報収集後、流出など、5つの主要特徴を持つ。



【図3】産業制御システムのターゲットSnakeランサムウェア

今年初めの注目すべきランサムウェア、Snakeが登場した。SnakeランサムウェアはGo言語を使用し、ランサムウェアによって暗号化されたファイル内の最後の部分に「EKANS」という文字列を追加するなど、自分だけの固有の特徴を表した。Snakeランサムウェアは典型的な産業制御システムのターゲットランサムウェアで、制御システムのOSがWindows基盤の各種生産機器をターゲットに攻撃を行う特徴を見せた。ユーザーの単純タッチのみを必要とするWindows基盤のHMI機器、データ保管サーバーなどを攻撃し、Windows OSでない機器は攻撃範囲に全く含まれなかった。

LockerGogaと同様に個人情報を徹底的に保証してくれるメールを使用したのが、Windowsのバックアップイメージを除去し、復元を完全に遮断したこと、暗号化後も遠隔でアカウント接続を維持したことは非常に特色ある部分だった。デジタル署名とマルウェア拡散のための自己拡散法を使用せず、組織内部拡散のためにAD（Active Directory）奪取などを行ったことは、彼らが単純なランサムウェア攻撃者ではないということの反証なのだろう。産業制御システムに対するターゲット攻撃にはランサムウェアだけでなく、様々な目的を持ったマルウェアが活用されており、攻撃範囲が次第に拡張している。一般ユーザーからの関心が比較的に少ない特殊目的のシステムに対するセキュリティシステムの構築及び管理が、そのいかなる時よりも重要な時期であることを忘れてはならない。

## 5.アダルトライブチャット・フィッシング

今年初め、n番部屋事件で全国が騒がしかった。5月20日にはn番部屋防止法案が国会を通過し、ネット業者にはデジタル性犯罪の画像・動画を削除する義務が与えられた。非正常的な方法での脅迫は全世界人が解決すべき共通課題だが、依然として残存している問題だ。Webcam Backmailと呼ばれる脅威は、互いの素性を露出しない状態で行われるビデオ通話をする過程で、犯罪者が相手に多少過度な性的行為をするよう誘導し、それを録画した後動画を公開を口実に相手にお金を要求することをいう。

2000年代中盤までビデオ通話が流行し、2011年以降スマートフォンのランダムチャットの領域に入ってから韓国国内ではアダルトライブチャット・フィッシングと呼ばれている。犯罪者はスマートフォンのランダムチャット中、音声、または画面がよく見えないという理由で特定アプリをインストールさせる。こうしてインストールされた悪性アプリによってスマートフォンに保存されている連絡先、メッセージ、写真などが流出して被害が発生した。攻撃者はこのウェブカメラの攻撃に加え、「連絡先に登録されている人たちに動画を流出する」と脅迫し、お金の要求までしたため、その恐怖が増幅したのだ。このような事件は思っている以上に多く、そして絶えることなく発生しており、家族や知人に流出するという脅迫に逆らうことができず、自殺に追い込まれることもかなり多く発生している非常に深刻なサイバー犯罪のうちの一つだ。

遠隔ビデオ会議の活性化により、2000年中盤以降消えていたウェブカメラが再び登場した今、セクストーション（Sextortion）の脅威がより強かになってくる可能性があることを記憶し、備えることが必要だ。Webcam Backmailの内容が含まれたメールを受信したら、動揺せずに落ち着いて内容に関わらず削除した後、気にしないことが重要だ。もし、それでも気になる場合、メールは削除して必要に応じて使用中のアカウント削除、パスワード変更、サービス退会などを考慮する必要がある。タイトルに自分が使用しているパスワードが含まれた状態でメールが送られてきた場合、現在の自分の個人情報状態を再確認し、同じパスワードは放棄することをお勧めする。これは、クラウドサービスの活性化によって特に気をつけなければならない部分だ。さらに、すべてのオンラインサービスがFacebook、NAVER、KakaoTalk、Twitterなどのアカウントを通してログインできるよう連携されている分、更なる注意が求められる。オンラインサービスログイン、またはスマートフォンログイン時に使用するIDとパスワードを徹底的に管理し、個人情報流出が疑われる場合、すぐに自分が使用しているパスワードを変更し、攻撃者が追加で攻撃を行えないようにすることが重要だ。

これまで、2020年上半期に登場した▲コロナ19を悪用したサイバーセキュリティ脅威の爆発的増加 ▲スミッシング&ボイスフィッシングの増加 ▲基盤施設ターゲットのマルウェア ▲OT&ICS領域まで忍び込んだランサムウェア ▲アダルトライブチャット・フィッシングなど、5つのサイバーセキュリティ脅威について調べた。

セキュリティ脅威は様々な社会的問題を悪用するため、政府機関及びセキュリティ会社で提供している様々な形の脅威情報に注意を払わなければならない。そして、自社のビジネス環境に合った対策を講じることで、より安全で自由なサイバー環境での活動が行えることを願いたい。



<http://jp.ahnlab.com/site/main.do>

<http://global.ahnlab.com/site/main.do>

<http://www.ahnlab.com/kr/site/main.do>



## アンラボとは

株式会社アンラボは、業界をリードする情報セキュリティソリューションの開発会社です。

1995年から弊社では情報セキュリティ分野におけるイノベーターとして最先端技術と高品質のサービスをご提供できるように努力を傾けてまいりました。今後もお客様のビジネス継続性をお守りし、安心できるIT環境づくりに貢献しながらセキュリティ業界の先駆者になれるよう邁進してまいります。

アンラボはデスクトップおよびサーバー、携帯電話、オンライントランザクション、ネットワークアプライアンスなど多岐にわたる総合セキュリティ製品のラインナップを揃えております。どの製品も世界トップクラスのセキュリティレベルを誇り、グローバル向けコンサルタントサービスを含む包括的なセキュリティサービスをお届け致します。

# AhnLab

〒108-0014 東京都港区芝4丁目13- 2 田町フロントビル3階 | TEL: 03-6453-8315 (代)

© 2020 AhnLab, Inc. All rights reserved.