アンラボ・セキュリティレター

Press Ahn

2022.3　Vol.99

2021 年に見られた Kimsuky グループの動向

2021 年に見られた Kimsuky グループの動向

多くの脅威分析アナリストらは「Kimsuky (キムスキー)」グループを、北朝鮮がバックについた国家支援型ハッカーグループと見ている。情報奪取を目的とする持続的標的型攻撃 (APT) グループとして知られており、2013 年 9 月、ロシアのセキュリティ企業である「Kaspersky (カスペルスキー)」によって、初めてその名が公表された。また、このグループによる活動は、現在に至るまで継続して行われている。

今回は、2021 年 1 月から 12 月までの間に確認された、Kimsuky グループの主な活動について説明する。

Kimsuky グループは 2020 年までの間、内部にマルウェアが挿入された hwp (ハングル) ファイルを流布する手法を主に使用してきた。しかし、2021 年頃からは、Microsoft Office 文書にマルウェアを挿入する手法へと移行している。現在も hwp (ハングル) ファイルを使用してはいるが、おとり文書 (正常ファイル) としてのみ活用する傾向にある。

月別に見てみると、2021 年 3 月頃から、原稿作成に対する所定の謝礼金を支給するとの名目で、金銭関連の内容を用いたマルウェアが大量に流布された。

また 6 月には、韓国内におけるエネルギーおよび航空宇宙産業分野へのハッキング事件に関し、バックで動いているのが Kimsuky グループであるとも報道された。VPN の脆弱性を利用し、内部に侵入したと伝えられているが、詳細な部分は明らかになっていない。

同じく 6 月には、特定の団体や人物を詐称したスミッシング攻撃が仕掛けられ、韓国インターネット振興院 (KISA) のモバイルワクチンに偽装した APK (Android Application Package) ファイルが流布された。この APK をインストールし実行してしまうと、端末内の機密情報が奪取され、C&C サーバーに転送される。これにより、攻撃者側はユーザー端末の遠隔操作が可能になる仕組みだ。

[図 1] APK ファイル実行時に表示される画面

さらに、2021 年も新型コロナウイルスの感染拡大が終息することなく続いたことで、関連トピックを悪用したマルウェアも度々流布された。

攻撃手法の面においては、不正 hwp (ハングル) ファイルから 不正 Microsoft Office 文書を利用した流布に移行しているものの、以前から使用されてきたタイプのマルウェアや攻撃手法も並行して活用している。ただし、少しずつではあるが、新しいタイプのマルウェアを使用し、暗号化方式や文字列などに変化を加える動向も見られる。また、比較的最新の脆弱性を利用した攻撃を敢行してくるケースも確認された。

尚、攻撃頻度別で見てみると、原稿作成に対する所定の謝礼金支給を名目とする、金銭的な内容を扱ったマルウェアの流布が最も多かった。金銭に関する内容なだけに、被害者を騙しやすいことがその理由と推測できる。攻撃対象を以前のものと比較してみると、国防や外交、南北統一に関する業務従事者という対象枠に大きな変化はなく、比較的最新の脆弱性 (CVE-2020-9715) を利用した攻撃が行われていた。この他にも、他グループが使用するマルウェアを用いることで、アナリスト達に混乱を与えたりもした。

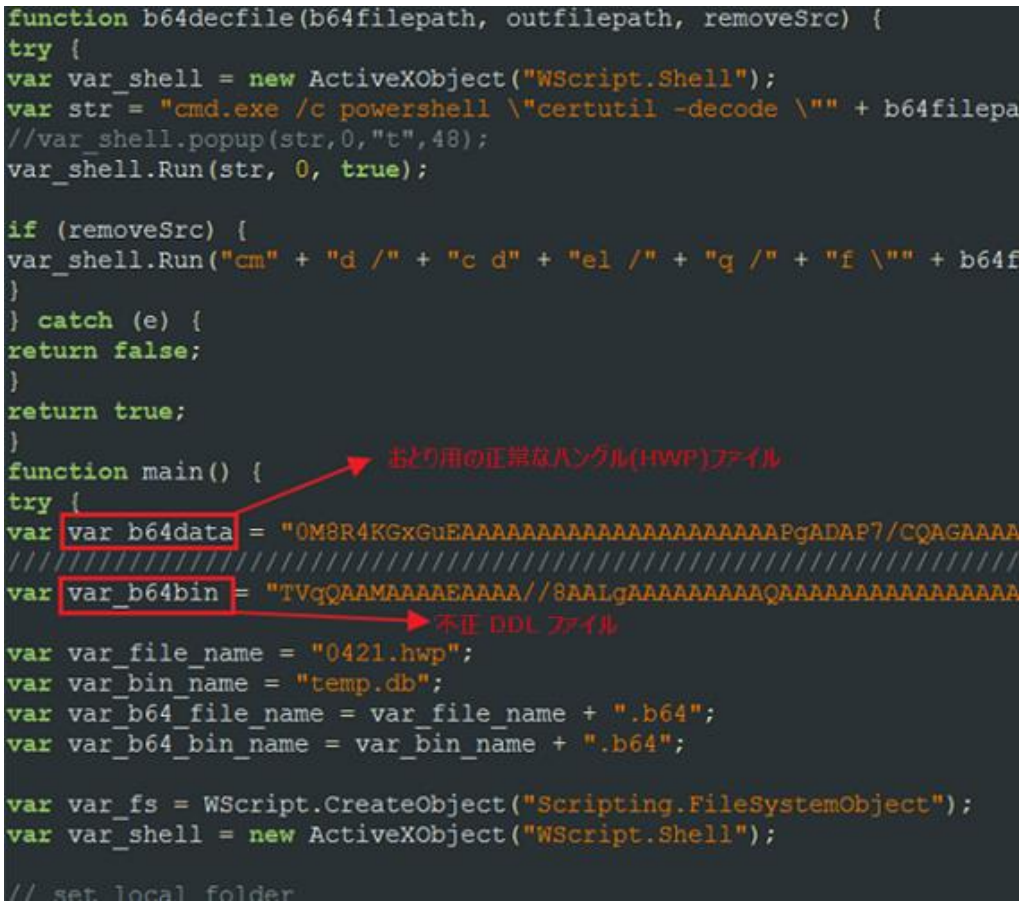
要約すると、Kimsuky グループは 2021 年に様々なタイプの攻撃を活発に、高頻度で行ってきた。そんな彼らの活動は、今後も引き続き行われることが予想される。

Kimsuky グループが使用する主なマルウェア

先に述べたように、Kimsuky グループは主に、以前から使用してきたマルウェアを再利用する手法をとっている。しかし、時折マルウェアを変形させたり、新しいタイプのマルウェアを用いて攻撃を行う場合もある。これに関し、2021 年に使用された主な変型および新型マルウェアを調べてみた。

#タイプ 1 : AppleSeed (JavaScript バージョン)

AppleSeed (アップルシード) は、システム情報を収集し、C&C サーバーから受信したコマンドに従い、悪意ある行為を行う backdoor (バックドア) 形態のマルウェアだ。主に実行ファイル (EXE) からのみ流布されていたが、JavaScript を介して流布されるケースもある。実行時は、おとり用の hwp (ハングル) ファイルや、不正 DLL ファイルを BASE64 デコードし、ドロップ後に実行する仕組みだ。



[図2] AppleSeed をドロップする JavaScript

おとり文書の内容からして、外交部関連の従事者を対象に攻撃を仕掛けているものと推測される。ちなみに、 2021 年に流布されたマルウェアのうち、流布量が最も多かったのがこの AppleSeed である。

#タイプ 2 : AppleSeed (Android APK バージョン)

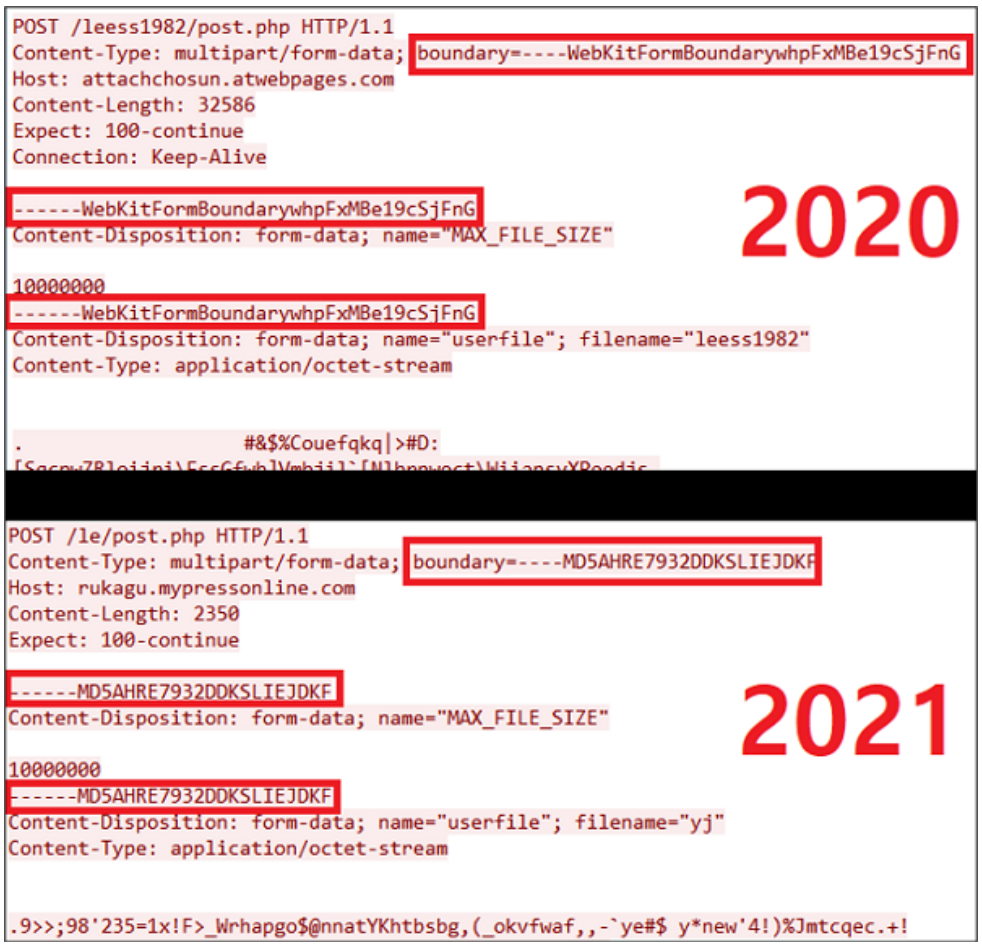
AppleSeed の事例のうち、KISA のモバイルワクチンに偽装した APK ファイルの流布も確認されている。この APK ファイルをインストール後に実行すると、ログイン資格証明および機密情報を収集し、C&C サーバーに転送することで、様々な悪意ある行為が行われる。

[図3] AppleSeed APK コードの一部

この APK に用いられるアルゴリズムは、Windows AppleSeed に使用されるアルゴリズムと 100% 一致する。

#タイプ 3 : FlowerPower (Powershell スクリプトベースのキーロガー)

FlowerPower (フラワーパワー) は、PowerShell (パワーシェル) スクリプトベースの Keylogger (キーロガー) である。システム情報を収集し C&C サーバーに転送することで、継続的にキーロギングを行うタイプのものだ。ちなみにキーロギングとは、ユーザーがキーボードを介して入力した内容を、密かに傍受し記録することを意味する。



[図4] 2020 VS 2021 のサンプル比較

機能面については以前と変わらないものの、通信時に別の文字列を用いる新しいタイプが確認されている。サンプル全てに変更した文字列が使用されているわけではなく、以前と同じ文字列を使用したサンプルと、混合して活用されていることが推測される。

#タイプ 4 : PDF エクスプロイト (CVE-2020-9715)

その他にも、「Use-After-Free」の脆弱性を利用した不正 PDF 文書が配布された事例もある。これは、解除されたメモリにアクセスし、コード変更を可能にするタイプのマルウェアだ。この PDF 文書が実行されると、内部に含まれた不正 JavaScript が機能し、外部から追加ファイルをダウンロードし実行する仕組みとなっている。

[図5] PDF 内部に含まれた不正 JavaScript

分析当時の追加ファイルは確保できなかったものの、おとり文書の内容を見る限り、南北統一に関する業務従事者を狙ったものと推測される。これ以外にも、同様の脆弱性を利用し、計算機のみを単純に実行する文書も発見されたが、これは脆弱性のテスト目的で作られた文書とみられている。

#タイプ 5 : PebbleDash (バックドア型)

PebbleDash マルウェアは、「Lazarus (ラザルス)」グループが使用することで知られており、2016 年からその存在が確認されてきた。また、Kimsuky グループによる PebbleDash マルウェアの使用事例は、2021 年 9 月に初めて報告されている。

```
v5 = sub_140001130("8QLnXjY0bgkb9GEb94eR9E"); // GetModuleFileNameW
if ( !(v5)(hInstance, v69, 1024i64) )
  return 0;
v6 = sub_140001130("nPgpDoispyzwbyj");         // CreateFileW
v7 = (v6)(v69, 0x80000000i64, 3i64, 0i64, 3, 128, 0i64);
if ( v7 == -1 )
  return 0;
v8 = sub_140001130("ZyG2eE2J9_W8Eb_Mu5");      // SetFilePointer
(v8)(v7, 4294966764i64, 0i64, 2i64);
v9 = sub_140001130("2AG8l3TqJ4x9");            // ReadFile
(v9)(v7, &v56, 532i64, v59, 0i64);
v10 = v56;
v11 = sub_140001130("SQVpUcbs3U5VOA");         // LocalAlloc
v12 = (v11)(64i64, v10);
if ( !v12 )
{
  v13 = sub_140001130("_F-4IgsWPdb9ngg");      // CloseHandle
  (v13)(v7);
  return 0;
}
```

[図 6] 暗号化された文字列

```
  while ( v7 );
  v8 = 0i64;
  v9 = v2 - 4;
  if ( v9 )
  {
    do
    {
      v10 = 0i64;
      while ( result[v8] != KeyTable[v10] )
      {
        if ( ++v10 >= 0x40 )
          goto LABEL_18;
      }
      result[v8] = KeyTable[(v10 - *(v11 + 2 * (v8 & 3))) & 0x3F];// zcgXlSWkj314CwaYLvyh0U_odZHBOReKiNIr-JM2G7QAxpnmEVbqP5Tu09Ds6fFt
LABEL_18:
      ++v8;
    }
    while ( v8 < v9 );
  }
  return result;
}
```

[図 7] 復号化アルゴリズム

PebbleDash は、情報収集と奪取コマンドを実行するバックドア型のマルウェアである。内部に含まれた KeyTable (キーテーブル) を使用し演算することで、全ての文字列の復号化が行われるよう機能している。

#タイプ 6 : BravePrince (変型 1 / 変型 2)

BravePrince は基本的にシステム情報の収集し、遠隔サーバーへの転送機能が備わっている。さらに、ファイル内に含まれた ID・パスワードを活用し、韓国のメールサーバーを介して、収集した情報とキーロギングによるデータを送信する変型も発見された。(変型 1)

2017

```
{
  int v2; // esi

  if ( !CreateMutex_4010E0() )
  {
    sub_10012B60();                     // ADD Reg
    v2 = rand() % 300 + 300;
    while ( 1 )
    {
      Sleep(1000 * v2);
      v2 = rand() % 900 + 1800;
      sub_10013A30();                   // Process Hollowing
    }
  }
  return 0;
}
```

2021

```
{
  int v1; // esi
  int v3; // [esp+0h] [ebp-Ch]
  int v4; // [esp+4h] [ebp-8h]

  if ( !CreateMutex_4010E0() )
  {
    sub_40AB50();
    Sleep(0x3E8u);
    CreateThread(0, 0, StartAddress, 0, 0, 0);
    if ( !sub_40CBA0() )                // Check Port(3389)
      sub_40C680();                     // Connect C&C Server
    v1 = rand() % 300 + 300;
    while ( 1 )
    {
      Sleep(1000 * v1);
      v1 = rand() % 900 + 2700;
      sub_40B4A0(v3, v4);               // Process Hollowing
    }
  }
  return 0;
}
```

[図8] 過去のタイプと新たに確認された変型との比較

BravePrince は本来、メールサーバーを介してのみ特定のメールに情報を送信していた。しかし、変型 1 では、メールサーバーに転送する前に、3389 番ポートが開いているかを確認し、閉じている場合 C&C サーバーと通信することで、追加ファイルのダウンロードおよび実行を行うルーティンが追加されている。

[図9] 暗号化方式の比較

さらに、前述した PebbleDash の暗号化方式を用いた BravePrince の変型も 9月に発見された。(変型 2) 従来の PebbleDash に使用されているキーテーブルのコードに変化はないが、アルゴリズムだけが少々変化しており、また BravePrince にはマイナス演算が用いられるが、PebbleDash にはそれがみられなかった。

終わりに

2021 年、Kimsuky グループの攻撃に使用された主なファイル名と形式は、[表 1] の通りである。

バイデン政権発足企画アンケート.doc
謝礼金支給依頼書.doc
謝礼金支給依頼書(テンプレート).doc
謝礼金支給依頼書.docm
企画アンケート.doc
[アンケート] 2021 データベース未来予測研究_(平和安保).doc
1. 2021 年事業計画 (施設本部資料参考補足) - 210316-1.pif
北朝鮮非核化コントロールタワー構築(案).wsf
AutoUpdate.dll
バイデン行政部安保ライン.wsf
アメリカ、日韓紛争仲裁の模索.doc_

[表 1] 2021 年 Kimsuky グループの攻撃に使用された主なファイル名

韓国内だけでなく、世界中から注目されている Kimsuky グループは、2021 年の 1 年間に、様々な手法や戦術を用いて活発に攻撃を仕掛けてきた。こうした動向は今年も続くとみられ、昨年確認されたものと同じような変型マルウェア、もしくは新しいタイプのマルウェアを活用することが予想される。ユーザーは、今回の記事でまとめた Kimsuky グループの主な攻撃手法や、攻撃に使用されたファイル名を把握し、類似した攻撃による被害に備え、事前に予防すべきである。

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)