アンラボ・セキュリティレター

Press Ahn

2019.9　Vol.69

Operation Moneyholic 詳細分析

仮想通貨を狙う標的型攻撃をプロファイリング

Operation Moneyholic 詳細分析

相場の乱高下により不安定な状態が続いているにもかかわらず依然仮想通貨(Cryptocurrency)への関心は熱い。価格上昇への期待と匿名性から追跡が難しいため、攻撃者らも仮想通貨を獲得すべくランサムウェアやコインマイナー(Miner、またはCoin miner)、Cryptojackingなど様々なタイプのマルウェアを作成・拡散させている。また仮想通貨取引所への攻撃や仮想通貨ユーザーアカウントのハッキングも珍しくなく、2018年になると韓国の仮想通貨取引所と利用者を狙うマルウェア攻撃が継続的に展開されている。アンラボセキュリティ対応センターは、仮想通貨を狙う一連の攻撃を『オペレーション・マネーホリック(Operation Moneyholic)』と命名し、プロファイリングレポートを発表した。

アンラボセキュリティ対応センター(AhnLab Security Emergency response Center、以下ASEC)では多数の仮想通貨関連マルウェアを分析したところ、標的型攻撃が疑われる一連の活動を捉えた。ASECが「オペレーション・マネーホーリック(以下、Moneyholic)」と命名したマルウェアの活動と脅威グループを追跡・分析した結果、攻撃ターゲットは仮想通貨取引所と利用者に絞られた。また数年に渡って韓国で標的型攻撃を展開した特定の脅威グループとの関連状況も明らかになった。

Moneyholicは主にメールを通じてマルウェアを配布していた。注目すべき部分は Moneyholicが 2018年2月から 2019年8月現在までマルウェアの作成・配布方法を常に変化させてきたという点だ。今回のプレスアンでは、Moneyholicの特徴を詳細に紹介した。

二重拡張子とスペースを利用したファイル名

Moneyholicは 2018年初めから中後半までメールに添付されたファイル名に二重拡張子を使用したり、意図的にスペースを含めた。実行ファイルであることを隠してユーザーの疑いを避けるための手法で、[表1]のようにファイル名に文書ファイルのフォーマット拡張子(.xlsx、.hwpなど)を入れて文書ファイルに偽装していた。ファイル名に仮想通貨関連(コイン、BCOTなど)の内容が入っていることも目を引く。

	ファイル名
1	WXBコイン　割合内容の件_送付用.xlsx.　　exe
2	***グループ3次-5次BCOT購入リスト及び数量確認(最終版).hwp.exe

[表1]二重拡張子とスペースを使用したファイル名

ユーザーが文書ファイルのように装った添付ファイルを実行すると、まずマルウェアが作動する。その後多数のマルウェアを追加ダウンロードするが、バックドア機能を実行する『TiWorker.exe』も一緒にダウンロードされる。TiWorker.exeはソースコードが公開された中国産バックドアをベースに製作されたもので C&Cサーバーと通信して特定のシグネチャ(fxftest)を送信する。

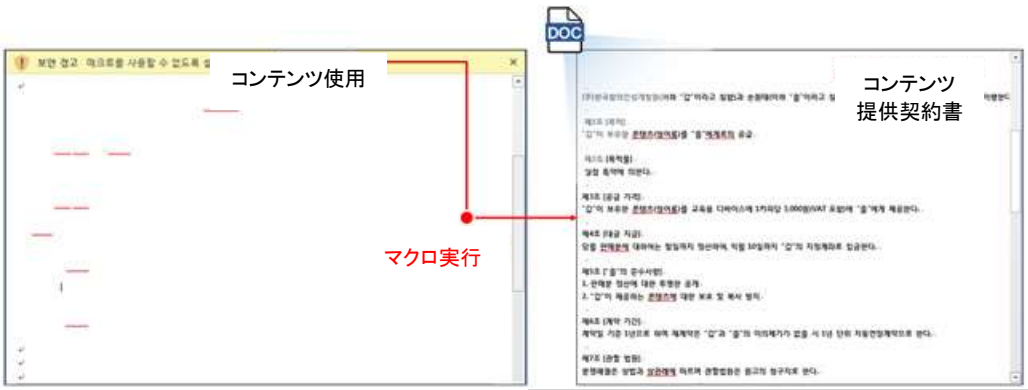
[表1]の hwp(ハングル)形式文書に偽装した『~BCOT購入リスト~.hwp.exe』が追加マルウェアをダウンロードする C&Cサーバーアドレスには、不正ファイル3つとともにユーザーの疑いを避けるための偽装用の正常ファイル 8個も存在していた。偽装用ファイル中、BASE64で暗号化されたファイルを復号化すると仮想通貨イーサネットリウム(ETH)関連内容の hwpハングルファイルが表示されるが、ファイルの作成者情報に「ASPNET」というアカウントが使用されていた。同ファイルのほか、残り 7つの偽装用ファイルを最後に保存したアカウントも ASPNETだった。攻撃者が ASPNETアカウントでログインした後、1個の偽装用文書ファイルで 7個の異なる内容の文書ファイルを作成したことが推測できる。

「ASPNET」は TiWorker.exeが追加ダウンロードしたマルウェアによって感染 PCに作成されたリモートデスクトッププロトコル(Remote Desktop Protocol、以下RDP)アカウントだった。攻撃者は RDPアカウントを介して外部から感染 PCに接続して悪質な行為を行うことができる。アンラボの分析結果、攻撃者は RDPアカウントで感染 PCに接続してパスワードを変更したことが分かった。

[図1] 感染 PCに作成された RDPアカウント(ASPNET)

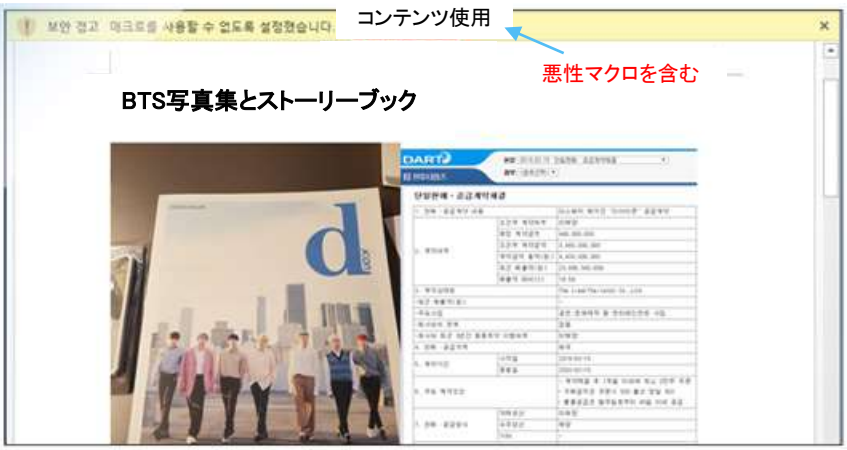
多様な手法で偽装用の文書ファイル作成

Moneyholicはユーザーの疑いを避けるために 2018年後半からマクロ、文書の脆弱性(OLE/Cve-2017-8570等)、MS Wordの正常な機能である DDE(Dynamic Data Exchange)を悪用するなど、多様な手法で偽装用文書ファイルを作成した。マクロを利用した際に、悪意あるマクロを含むシートを非表示にしたり、[図2]のように「コンテンツ使用」ボタンをクリックするように誘導した。



[図2] 「コンテンツ使用」ボタンのクリックを誘導して悪性マクロを実行

攻撃者は社会工学的手法(Social Engineering)を利用して攻撃の成功率を高めた。一例として、[図3]のように人気アイドルグループに関する内容に偽装した悪意ある圧縮ファイルを配布したケースもあった。



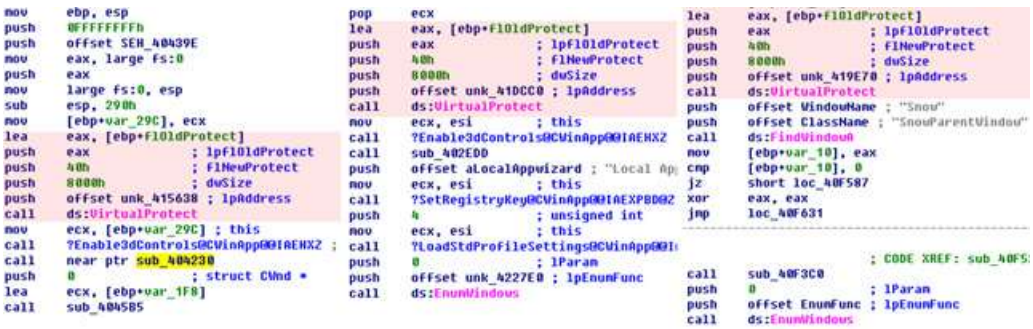
[図3] 人気アイドルグループ関連コンテンツに偽装した不正ファイル

アマデイ(Amadey)バックドアの登場

2018年下半期以降は顕著な変化が現れた。アマデイ(以下、Amadey)と呼ばれるボットネット(Botnet)を使用したマルウェアである。BASE64で暗号化された txtファイル(cabファイル)を復号化すると、Amadeyが含まれていることが確認された。

Amadeyはロシア開発者が制作したことで知られるボットネットマルウェアで、攻撃者は同マルウェアに感染したシステムで必要なファイルをダウンロード実行するタスクコマンドを送信したり、感染システム情報を確認した。

Moneyholicが配布した Amadeyは、見た目は正常ファイルになりすましている。ファイル形式で存在するため実行もできるが、実際にはメモリ上で実行ファイルに再構成されてバックドアの役割を担う。Moneyholicの Amadeyは[図4]の赤く塗りつぶされた部分のような共通点を持つが、Virtual Protect()で保護された領域に存在するデーターは暗号化されたシェルコード(Shellcode)と Amadeyで構成されている。



[図4] Amadeyの共通的な特徴

Moneyholicの Amadeyは主に C&Cアドレスやアンチウィルスの名前を文字列として使用しており、感染 PCに当該アンチウィルスがインストールされているかどうか確認し、その結果をフラグ(Flag)に設定して C&Cサーバーに送信する。送信内容は [図5]のように Amadey管理者メニューの「AV」タブに表示されていた。

[図5] Amadey管理者メニューに表示された感染 PCのアンチウィルス

Amadey変種と C&Cサーバーが通信したパケットを分析したところ、Moneyholicは感染 PCのプロセスリストで仮想環境に関するプロセスが実行中の場合、マルウェア分析用の PCであると判断して、分析を妨害するために MBR破壊マルウェアを追加でダウンロードすることが確認された。感染 PCに仮想通貨関連のデーターが存在すれば、これを奪取するマルウェアも追加でダウンロードする。

攻撃範囲の拡大(2019年上半期)

2019年5月から配布されたマルウェア(cab)には従来と同じバックドア(TIWorker.exe、ipnet.dll、Amadey)が存在しなかった。代わりに OSでサポートするコンソールコマンドを利用して感染 PCのファイルとフォルダーリスト、OSとハードウェア情報などを収集するバッチファイルと、収集した情報を C&Cサーバーに送信する実行ファイル(Sendfile.exe)が存在していた。

その他の変化としては、既存の Windows用マルウェアだけでなく Android向け悪意あるアプリを作成・配布し始めたという点だ。悪意あるアプリは Windows用のマルウェア配布サーバーから発見された。同アプリが実行されるとまず感染システム状況を確認するが、もし PC環境ならば『モバイル環境でのみインストールできます』というメッセージを表示する。Android スマートフォンにインストールされたことを確認すると、不正アプリのダウンロードリンクに接続する。ダウンロードされた悪意あるアプリはユーザーの疑いを避けるためにアイコンを非表示にした後、バックグラウンドで情報奪取など悪質な動作を起動していた。

Moneyholic の背後に潜むもの

2018年2月から 2019年8月までに配布されたマルウェアをプロファイリングした結果、数年かけて韓国の主要機関や企業を対象に標的型攻撃を展開した『キム・スキー』と呼ばれる「Kimsuky」グループと Moneyholicの関連性が確認された。

2018年2月に発見された感染 PCの中から多数のマルウェアが確認されたが、その中に Utilman.exeファイルがあった。同ファイルは 2017年2月にも発見され、当時 Utilman.exeと一緒に発見されたキーロガーが 2013年に Kimsukyグループが使用したキーロガーと同じだった。また Kimsukyグループが 2017年8月から使用したマルウェアに感染した PCからも、Utilman.exeと同じような機能を持つマルウェアが発見された。

別のケースとしては 2019年5月24日、主要アンチウィルスをベースにマルウェアスキャンを提供する VirusTotalサイトで Kimsukyグループが配布したファイル(「Huobi Research Weekly(Vol.62)2019.05.13-2019.05.19.doc」、以下Huobi Research.doc)が見つかった。

Moneyholicが使用した C&Cサーバーアドレスが Huobi Research.docファイルも同じように存在していたがコメントアウトされており、新しい C&Cサーバーの naoei3-tosma.96.ltが追加された。また同ファイルのプロパティを確認したところ作成日時と作成者が同じであることが分かった。

[図6] Moneyholicファイル(上)と Kimsukyグループファイル(下)の不正マクロを比較

ほかにも複数の関連性に基づいて推測できるのは、2月にアンラボが「Operation Kabar Cobraレポート」を通じて述べたように Kimsukyグループをはじめ、韓国で標的型攻撃を展開している攻撃者の場合、金銭的利益の拡大に集中しており、これにより攻撃範囲がさらに拡大する可能性が高いということだ。

Moneyholicに関するより詳細は ASECが発表した「Operation Moneyholic : 金銭的利益を目的とした最新の標的型攻撃事例」レポートで確認することができる。

▶「Operation Moneyholic」分析レポートのダウンロードはこちらへ(現在韓国語版のみ)

関連レポート:

▶「Operation Kabar Cobra」分析レポートのダウンロードはこちらへ(英語版)
▶「Operation Kabar Cobra」分析レポートのダウンロードはこちらへ(韓国語版)

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)