アンラボ・セキュリティレター

Press Ahn

2019.7　Vol.67

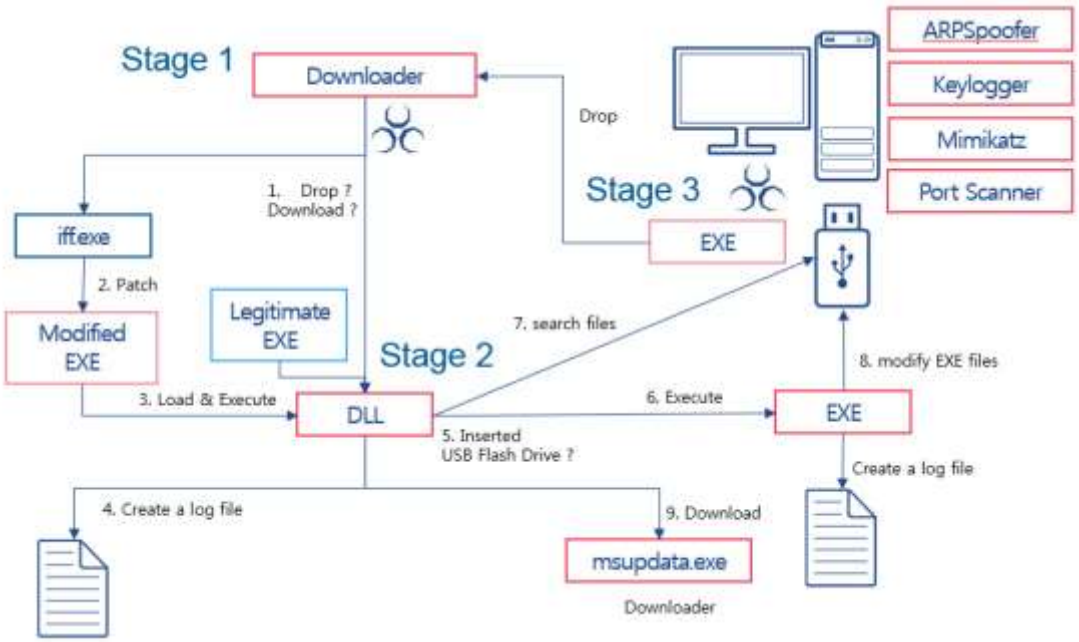
USB を狙う攻撃、そのコアにあるもの

Tick グループ攻撃手法の詳細分析

USB を狙う攻撃、そのコアにあるもの

2008年以降防衛産業をはじめ国防および政治関連機関、セキュリティ、IT、電子など多様な産業分野を対象に攻撃を展開してきた脅威グループが存在する。「ティック(Tick)」グループと呼ばれる同グループは、攻撃対象の脆弱性を事前に把握して、さまざまな方法を利用して継続的な攻撃を仕掛けている。特にここ数年間は韓国企業の内部情報を奪取するために企業で使用するセキュリティ USB を利用したマルウェア感染を試みた。アンラボセキュリティ対応センター(AhnLab Security Emergency-response Center、以下ASEC)は最近発表した ASECレポート(ASEC Report Vol.95)で USBを狙ったマルウェア「Tickusb」について攻撃手法を詳細に分析した。今回のプレスアンでは Tickusb 攻撃に使用された主なマルウェアを紹介する。

「Tickusb」とは Tick攻撃グループが USBを通じて企業の機密情報などを流出するために製作したマルウェアで、2014年春から 2017年冬まで継続的に様々な変形が発見された。[図1]は Tick攻撃グループが使用した Tickusbマルウェアの関係図だ。まず不正 DLLファイルが実行されると特定のパスにログファイルを作成して USBの接続をチェックする。システムに USBが接続されている場合、悪意ある EXEファイルを実行して追加ファイルをダウンロードさせる。悪意ある EXEファイルは変形タイプによって少しずつ異なる機能を実行するが、一般的には USBファイル情報を収集する。一部の変形は USB内の EXEファイルを改ざんし、改ざんされた EXEファイルを持つ USBを別のシステムに繋げて同ファイルを実行するとそのシステムも Tickusbマルウェアに感染されてしまうのだ。



[図1] Tickusb マルウェアの関係図

Tickusbマルウェアの構成

単独ファイルとして存在するものもあるが、ほとんどの Tickusbマルウェアは DLLファイルと EXEファイルで構成されている。

1. DLLファイル

Tickusbマルウェアの DLLファイルは、BrWeb.dll、CRYPTBASE.dll、wincrypt.dllなどがある。これらの DLLファイルはローダー(Loader)の役目を担い、[図2]のように実行するログファイル名、EXEファイルパス、ドライブタイプなどの文字列を含む。

[図2] DLLファイルの主な文字列

しかし、2015年4月に発見された Tickusbマルウェアは DLLファイルの単独タイプであり、追加の EXEファイルが存在しなかった。また2015年6月に発見された BrWeb.dllは Brotherプリンター関連ファイルに偽装し、プリンター関連ファイルの BrStMon.exeをパッチして、EXEファイルが実行されるときにロードされていた。

2. EXEファイル

Tickusbマルウェアの EXEファイルは USBのファイルリストを収集したり、EXEファイルを改ざんすることもあった。cftmon.exe、svcmgr.exe、wsmt.exe などが確認されており、これらの EXEファイルには [図3]のようにファイル感染に関連する文字列、USBに関するログの文字列が含まれていた。

[図3] EXEファイルの主な文字列

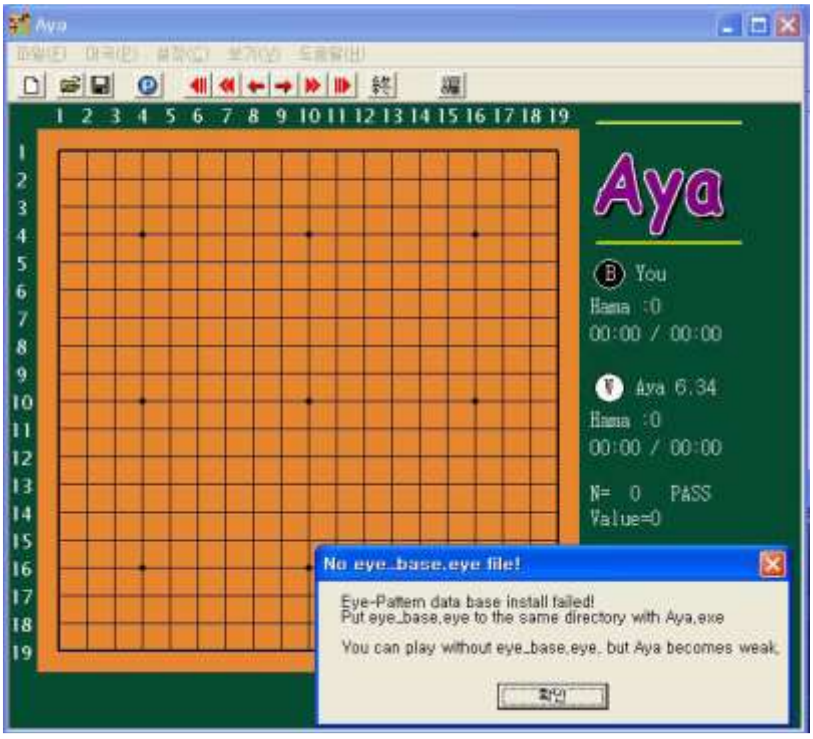
2015年6月に発見された EXE変形は、USB内のファイル情報を収集して EXEファイルを改ざんする機能が追加され、改ざん対象の EXEファイルの末尾に特定のファイルを追加して実行させる手法を使用した。2012~2014年までに発見された一部変形では、韓国の企業で使用する特定のセキュリティ USBが接続すると 同 USBの特定の領域からデータを読み取って実行することが確認された。これはネットワークの分離環境システムを攻撃するためのものと推定される。

関連マルウェアの詳細分析

Tickusbマルウェアの詳細な感染方法はまだ把握しきれていないが、これに関するドロッパー、ダウンローダーなどは発見済みである。ドロッパーを通じて改ざんされたインストールファイルと、 Tickusbマルウェアに感染した USBに存在するファイル改ざんコードを比較した結果、ドロッパーの一部は Tickusbマルウェアが改ざんした EXEファイルであることが確認された。また攻撃者は Windows起動時に Tickusbマルウェアが自動実行されるようにする代わりに、特定のファイルが実行される時のみ動作されるようにした。これはユーザーがマルウェア感染の有無を把握できないようにするためと思われる。

1. ドロッパー(Dropper)

Tickusbマルウェアに関する多数のドロッパーが存在するが、アンラボが 2014年3月に収集した Aya.exeもその一つである。Aya.exeは囲碁ゲーム関連ファイルで、[図4]の囲碁ゲームが実行されると一時フォルダーに初期バージョンの Tickusbマルウェアが作成される。この他にも 2015年6月初めに発見された Secure Unlock win.exe、Portable SecretZone.exe、pNDPS(V2.11).exe、NEW_GOMPLAYERSETUP.exeなどのドロッパーが確認された。



[図4] Aya.exe実行画面

2. ダウンローダー(Downloader)- ゴーストダウン(Ghostdown)

Tickusbマルウェアに感染したシステムからダウンローダーの役目を担う Ghostdownが確認された。Ghostdownは 2013年2月に登場して以来 2018年2月まで活動が確認され、変形も発見されている。[図5]は Ghostdown変形で確認された文字列で API、接続アドレスなどの主要文字列が暗号化されている。初期バージョンの Ghostdownは接続アドレスと主要文字列が XOR 0xDF キーで暗号化されていた。また初期の変形は www.dnserver.comという C&Cサーバーを使用していたが、2016年に感染システムから発見された Tickusbマルウェア変形はクラウドサービスを利用したことが確認された。

[図5] Ghostdown変形の文字列

3. パッチャー(Patcher)- iff.exe

iff.exeは EXEファイルを改ざんして特定の EXEファイルを実行したり、特定の DLLファイルをロードする。Tickusbマルウェアに感染したシステムで検知された iff.exeファイルは、攻撃者がシステムに侵入した後で追加インストールしたファイルと推定される。

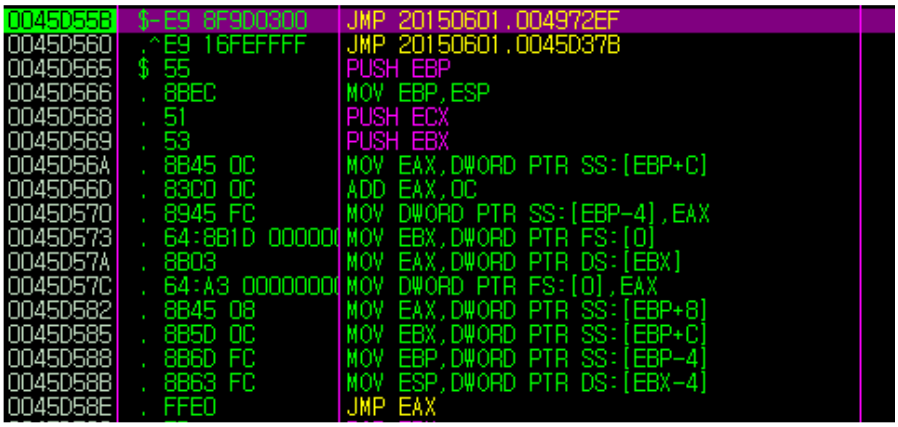
iff.exeは、改ざん方式、改ざん対象ファイル、実行ファイルやロードする DLLファイルを引数で入力する。またプログラムの開始位置である Entry Pointへのジャンプコマンドを変更して、iff.exeが追加したコマンドが先に実行されるようにする。

[図6] iff.exe 実行画面

4. ローダー(Loader)- BrStMonW.exe

2015年6月1日、攻撃者は iff.exeファイルを利用して Brother社のプリンタープログラム「BrStMonW.exe」をパッチした。BrStMonW.exeを実行すると、悪意ある BrWeb.dllファイルを先にロードするように改ざんしたのだ。また [図7]のように同マルウェアが追加したコードアドレス「0x004972EF」が最初に実行されるように Entry Point を修正した。

iff.exeのような Patcherを使用すると、攻撃者はシステム侵入後にプログラムを選択してパッチを実行、追加のマルウェアを実行するように仕向けることができる。特徴は BrStMonW.exeの空の領域に任意のコードを上書きするため、ファイル改ざん後もファイルの長さに変化がないということだ。iff.exeによって追加されたコードは特定の DLL(BrWeb.dll)ファイルをメモリにロードして実行する。つまりプリンターを使用する時のみ Tickusbマルウェアが動作するためユーザーが感染に気付くのは難しい。



[図7] 変更された Entry Point

追加インストールファイル

Tickusbマルウェアに感染したシステムからはキーロガー(Keylogger)、ARPSpoofer、Port Scanner、Mimikatzなども追加で発見されている。

1. キーロガー(Keylogger)

Tickusbマルウェアに感染したシステムの一部からキーロガーが発見された。2017年4月から 2018年2月までに発見されたキーロガーは主に apphelp.dll、linkinfo.dll、netutils.dllなどのファイル名を使用し、ユーザーが入力したキー内容を debug.logに保存していた。

2. ARPSpoofer- hwp70.exe

攻撃者は韓国で使用されるハングルプログラム関連ファイルに偽装して攻撃を実行した。Tickusbマルウェアに感染したシステムの HancomOfficeフォルダ(C:¥HNC¥Hwp70)から不正ファイルの hwp70.exeが見つかっている。

3. Port Scanner

攻撃者は 2016年に Foundstoneのポートスキャナーである ScanLineをパッキングしたファイルを攻撃に利用した。多数のシステムで同プログラムを使用したことが確認されており、使用されたファイル名は msp.exe、ls.tmp、sl-p.exeなどであった。

4. Mimikatz- mi.exe、mi2.exe

攻撃者は感染システムに Mimikatz変形「mimi 2.1」と「mimi 2.1.1」バージョンを使用した。ファイル名も Tickグループで主に使用する mi.exe、mi2.exeだった。

Tickグループ、攻撃対象のインフラに応じて攻撃手法を選択

2008年から約 10年にわたり機関や企業を継続的に攻撃している Tickグループは、攻撃対象のシステム環境に応じて Spear Phishing、Watering holeなど多様な方法で攻撃を展開している。特に分離型ネットワーク環境などを攻撃するために USBの EXEファイルを改ざんしてマルウェアを感染させる方法を駆使するなど、閉鎖型やネットワーク分離環境を運用中の組織でも細心の注意が必要だ。

Tickusbマルウェアに関するより詳細な内容は、ASEC Report95号でも確認することができる。

▶「ASEC Report Vol.95」ダウンロード(英語版)

▶「ASEC Report Vol.95」ダウンロード(韓国語版)

V3シリーズでは Tickusbマルウェアを次の診断名で検知している。

<V3 製品群の診断名>

HackTool/Win32.Hijack

HackTool/Win32.Mimikatz

HackTool/Win32.Tickpatcher

Trojan/Win32.Agent

Trojan/Win32.Homamdown

Trojan/Win32.Loader

Trojan/Win32.Tickusb

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)