アンラボ・セキュリティレター

Press Ahn

2020.08　Vol.80

10 年間生き続ける、USB メモリ内の亡霊たち

USBメモリマルウェアの動向分析レポート

10 年間生き続ける、USB メモリ内の亡霊たち

セキュリティ業務に関わる人々であれば、普通は新しいセキュリティ脅威に対する動向や対応策に関心を寄せる。しかし、10年前に登場したUSB(Universal Serial Bus)メモリを通して広がるマルウェアの被害も依然として発生している。このレポートでは、USBメモリにより拡散するマルウェアの変化と特徴、技法と戦術、韓国内での活動について分析した。

USBフラッシュドライブは、国内では通常「USBメモリ」と呼ばれ、2000年に初めて販売を開始し、間もなく急速にフロッピーディスクに取って代わり、現在最も広く使用されているリムーバブルストレージメディアである。

フロッピーディスクよりも大容量で小さいサイズのため、内部資料流出などの問題が発生してUSBメモリの使用を制限した企業や機関も存在する。しかし、USBメモリの使用制限ポリシーは、ユーザーが不便さを訴えるため、すべてのシステムに適用するには無理がある。これらの理由により、一部機関や企業では例外ポリシーが適用されたシステムを運用することもある。

USBメモリによって広がるマルウェア被害は、次のような特定の分野において持続的に発生している。

- 製造産業(低仕様あるいは旧式システム)
- 特殊目的システム(ATM、POSシステム、キオスク)
- 公用システム(学校、図書館等)
- セキュリティポリシー例外システム等

製造産業分野では、生産工程に問題がない場合は従来のシステムを継続して使用しており、既にサポートが終了したWindows XPのようなオペレーティングシステム(OS)がいまだに使用されている。ハネウェル(HoneyWell)によると、USBメモリは、オペレーショナルテクノロジー(Operation Technology、OT)システムで2番目に広く使用されている産業ベクトルの脆弱性だという。産業界とATM、POSシステム、キオスク等の特殊目的システムも低仕様、旧式のオペレーティングシステムを使用しているシステムが運用されている。
これらの分野では、メンテナンスのためのプログラムやデータファイルをUSBメモリに入れてシステムに接続する過程でマルウェアに感染する事例が発生する。まだ国内では病院におけるマルウェア感染の報告は多くはないが、医療機器も旧式のオペレーティングシステムを使用している場合があり、注意が必要である。これらのシステムにはセキュリティプログラムが存在しない場合も多く、長い場合は数年間も感染した状態のままシステムが運用されることもある。

USB メモリ関連のマルウェアの進化

リムーバブルストレージデバイスに対する攻撃は、1980年代から始まった。1980年代と1990年代の初頭はフロッピーディスクによるブートが頻繁に行われ、フロッピーディスクがウイルス拡散の主な経路であった。今の時代にフロッピーディスクが使用されるのかとも思われるが、2019年まで核兵器を管理するシステムがフロッピーディスクにより運用されていることもあった。ハードディスクの普及によりフロッピーディスクによるブートは減少し、Windowsの時代へと移り変わると、ブートウイルスは急激に減少する。

1990年代半ば、CD-ROMの普及に伴って、オペレーティングシステムにもユーザーの利便性のため、記憶メディアを挿入すると指定したファイルの自動実行機能が追加された。しかし、攻撃者たちも自動実行機能を利用し始めた。1998年4月、マック(Mac)でQuickTime 2.0と自動実行(AutoPlay)機能を利用して拡散するオートスタート(AutoStart)ワームが広がった。このワームは韓国にも流入し、マック(Mac)用のアンチウイルスプログラムが製作された。CDメディアの自動実行機能と関連し、2005年10月のソニーBMG製CDに含まれていたWindowsルートキット(Rootkit)事件も有名である。

2000年にUSBメモリが発売されてから、フロッピーディスクを始めとする他のリムーバブルストレージメディアはその座を取って代わられた。読み取りと書き込みが可能な新しいリムーバブルストレージメディアの普及と自動実行機能は、マルウェアの製作者にとっても新たな機会となった。USBメモリにオートラン(Autorun.inf)ファイルを作成し、USBメモリがコンピュータに接続されるとマルウェアが自動的に実行されるワームが2006年に登場し、2007年からは本格的な問題になり始めた。

主なUSBメモリに関連するマルウェアの変化は、次の通りである。

日時	内容
2006年	自動実行(Autorun)機能を利用して拡散されるソロウ(Solow)等のワームが登場
2008年	セキュリティカンファレンスにおいて配布されたUSBメモリからマルウェアを発見
2008年11月	米軍、Agent.BTZマルウェアの被害を公開
2008年12月	SMBの脆弱性とUSBメモリの普及により拡散するコンフィッカー(Conficker)ワームの発見
2009年	難読化スクリプト型のワーム登場
2009年	情報流出型オートラン(Autorun)の発見。韓国で発見された変型は、HWPファイルも収集
2009年7月	Winows 7リリース。自動実行不可
2010年	スタックスネット(Stuxnet)の発見
2011年	標的攻撃においてUSBメモリの拡散機能を利用
2013年	USBメモリ内のファイル名のショートカット(LNK)ファイルを作成するワームの拡散
2014年	USBメモリ内の実行ファイルを感染させ、内部システムを攻撃するティックusb(Tickusb)の活動
2014年	USBメモリの拡散およびキーログ機能を持つドットロガー(Dotlogger)の発見
2016年	USBメモリ内のファイルやフォルダを特定フォルダに移動させ、同じ名前のLNKファイルのみを作成するワームの登場
2020年	USBメモリを利用して拡散またはUSBメモリ内の情報を収集するUSBferry、Ramsay、Compfun、USBCulpritマルウェアの発見

[表1] USBメモリを利用したマルウェアの変化

2006年に発見されたソロウ(Solow)は、ビジュアルベーシックスクリプト(Visual Basic Script、VBS)で作成されたスクリプトワームであり、最初に発見されたときはいかなる難読化もなかった。このワームは文字列が難読化されておらず、作成されたファイル名だけが多少異なったり、コメント等を追加した変型、ファイルコピー中に一部コードの変化等、様々な変型が発見された。
オートラン(Autorun.inf)ファイルを作成して拡散するマルウェアは、2007年から様々な種類が登場し、拡散し始める。2008年と2010年には、セキュリティカンファレンスで配布されたUSBメモリからマルウェアが発見され、国際宇宙ステーション(ISS)のコンピュータでもマルウェアが発見された。

2008年11月、米軍においてAgent.BTZワームが発見される。このマルウェアは2011年にも引き続き問題になった。このマルウェアは、特定国の支援を受けていると推定されるTurlaグループのマルウェアとして知られている。このマルウェアの最新バージョン4の変型は、2020年5月に韓国でも発見された。

2008年12月に発見されたコンフィッカー(Conficker)ワームの変型は、CVE-2008-4250(MS08-067)の脆弱性を利用して拡散する初期バージョンでオートラン機能を利用してUSBメモリでも拡散する。コンフィッカーワームは今でも産業界において最もよく見られるマルウェアで、MS08-067の脆弱性を利用して、接続した他のシステムも感染させる。これは、脆弱性が発見されセキュリティパッチが発表されたにもかかわらず、10年を超えるセキュリティ更新プログラムが適用されていないシステムが存在するため発生する問題である。

初期の頃は単純な拡散のみが行われる形だったが、一部のワームには情報流出の機能が含まれる。2009年に発見されたオートランワーム(md5: d81569c475154ddf7ab32ce7af393866)は、韓国のユーザーを標的としていた。このマルウェアは、システムでアレアハングルファイル(HWP)を含む複数の文書ファイルを収集する。この変型が作るオートラン(autorun.inf)ファイルには、「フォルダを開いてファイルを表示」、「開く」のようなハングルが含まれており、韓国語ユーザーを対象に製作されたと推定される。

2010年に発見されたスタックスネット(Stuxnet)は、USBメモリの脆弱性を利用して拡散する。LNK脆弱性(CVE-2010-2568)を利用し、Windowsエクスプローラのショートカットファイルが位置するディレクトリを開くだけでもショートカットファイルが自動で実行される。韓国国内においても、2011年にLNK脆弱性によって拡散するマルウェアを利用した標的型攻撃が発生したことがある。

USBメモリは、ネットワークから分離(air-gap)されたシステムでは、データのコピーに利用される。攻撃者はUSBメモリに主な資料が含まれており、USBメモリ内の情報を流出するマルウェアを製作した。このような攻撃方法は、2010年から試みが行われた。2010年、マルウェアに感染した状態でUSBメモリを接続すると、USBメモリのファイルを圧縮してネットワークに転送する機能を持つマルウェアが国内で発見されたこともあった。

2009年にリリースされたWindows 7から、CD-ROMを除くすべてのドライブのタイプにおいて、自動実行が不可能になった。新しいWindows OSの普及により、オートラン(autorun.inf)ファイルを利用した自動実行機能が使用できなくなると、マルウェアの製作者たちはオートラン(autorun.inf)ファイルの作成ではなく、ショートカット(LNK)ファイルを利用したワームを製作し、2013年以降はこれが一般化していった。これらのマルウェアは進化し続けており、単にLNKファイルを作成するのではなく、USBメモリ内のファイルやフォルダを.Trashesフォルダに移動させ、ファイルやフォルダと同じ名前のショートカットファイルに替わる(md5: 3f097745bc355e14961023392e369ed9)。このマルウェアは、システム設定を変更し、隠しファイルを見えないようにして.Trashesフォルダの属性を非表示にしてエクスプローラで表示ができないようにする。

2014年1月、インターネットに接続していない地域でも、USBメモリによって拡散するマルウェアが発見された。インターネットに物理的に接続されておらず、1週間に1度USBメモリにアンチウイルスプログラムのパッチファイルやエンジンファイル等のメンテナンスに必要なファイルを入れて使っていた時に発生した。

2014年、ティック(Tick)グループのティックusb(Tickusb)は、USBメモリを通して国内企業の機密情報等を流出しようとする目的で製作したマルウェアにより、2014年春から2017年11月までの活動が確認された。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、USBメモリの接続をチェックする。システムにUSBメモリが接続されている場合、不正なEXEファイルを実行し、追加ファイルをダウンロードすることもある。不正なEXEファイルは変型によって少しずつ異なる機能を実行するが、一般的にUSBメモリ内のファイル情報を収集する。一部の変型は、USBメモリ内のEXEファイルを改ざんする。最終的に改ざんされたEXEファイルがあるUSBメモリを別のシステムに接続した後でそのファイルを実行すると、そのコンピュータもティックusbに感染する。2015年4月には、ティックusbの変型であるCryptbase.dllが発見された。他のティックusbの変型とは異なり、DLLファイルの単独型である。Windowsの正常なCRYPTBASE.dllファイルと同じエクスポート(Export)関数を持っており、発見されたファイルのパスが%ProgramFiles%¥common files¥java¥java update¥cryptbase.dllとなっている。これにより、このマルウェアはJava関連プログラムが実行されるときに読み込まれたものと推定できる。

2015年6月1日に発生した攻撃では、DLLファイルとEXEファイルで構成された変型が発見された。攻撃者は、ブラザー(Brother)プリンタのドライバファイルであるBrSrMonW.exeをパッチし、そのファイルが実行されるときに不正なDLLファイルであるBrWeb.dllをロードするようにした。EXEファイルには、USBメモリからEXEファイルを検索して改ざんする機能が追加された。2016年10月には、Tickusbの変型であるwincrypt.dll(md5: 16572393021beea366679e80cc78610c)が発見され、同じファイル名を持つ変型は2017年11月まで確認された。

2014年6月から、ドットネット(.NET)で作成され、オートラン(autorun.inf)ファイルにより拡散するドットロガー(Dotlogger)が発見される。このマルウェアは、キーロガー機能が付随しており、2017年に発見された変型(md5: 664b3007c043c26cff911d8b400bd0bf)は韓国国内のアンチウイルスプログラムを停止させる機能を持っている。2016年以降に発見されたワームは、仮想通貨を発掘するコインマイナー(CoinMiner)と呼ばれるマルウェアをさらにダウンロードして実行することもある。

2020年にもトレンドマイクロ(Trend Micro)からUSBferry、イーセット(ESET)からRamsay、カスペルスキー(Kaspersky)からはCompfunとUSBCulprit等、USBメモリ内の資料を盗んだり、USBメモリを通してネットワークから分離されたシステムを狙ったマルウェアの情報が公開された。

USB メモリを悪用したマルウェアの技法と戦術

攻撃者は、マルウェアを拡散して自身を保護するために、複数の方法を使用している。

1.拡散 - autorun.infの作成

CD-ROMやUSBメモリにおいて、コンピュータに接続したときにオートラン(autorun.inf)ファイルが指定された特定ファイルを自動的に実行する機能を、Windows 95から対応した。攻撃者はこの機能を悪用し、リムーバブルディスクにオートランファイルを作成し、マルウェアが自動で実行されるようにした。

リムーバブルディスクにオートランファイルを作成して特定のファイルを実行するマルウェアは2006年(2005年以前も可能)に最初発見され、USBメモリ、メモリーカード、外付けHDD等のリムーバブルストレージデバイスにオートランファイルを作成する。オートランファイルにゴミデータの値を追加し、アンチウイルスソフトによる診断を妨げることもある。しかし、Windows 7以降では、もはやこの方法では自動的に実行されない。

2.拡散 - 実行の誘導

Windows 7以降のOSでは、オートランファイルを利用した自動実行機能が使用できなくなり、攻撃者は元々存在するファイルのショートカットファイルを作成したり、フォルダと同じアイコンの形を持つファイルを作成してユーザーのクリックを誘導するようになる。リムーバブルディスク内に存在するフォルダやファイル、或いはフォルダとファイルの両方を隠しファイル属性に変更し、フォルダやファイルと同じ名前のショートカットLNKファイルを作成する。ユーザーは、ショートカットファイルを元からUSBメモリに存在するファイルと勘違いしてクリックしてしまう。一部のマルウェアは、レジストリ内容を変更して「ショートカット」アイコンから矢印アイコンを削除し、ユーザーがショートカットだと判別しにくくする。

3.拡散 – USBメモリ内の実行ファイル感染

ネットワークから分離したシステムでも、ファイルコピーのためにUSBメモリが使用されることがある。一部のマルウェアはこの点を狙い、USBメモリ内の実行ファイルを改ざんして内部システムへの侵入を試みる。攻撃者は、インターネットに接続されたシステムにマルウェアを感染させ、USBメモリが接続されたときにUSBメモリ内のEXEファイルを感染させる。

USBメモリが外部と遮断されたシステムにおいて使用され、マルウェアが実行されると、情報を収集してUSBメモリに保存し、そのUSBメモリがインターネットに接続されたシステムで使用されるときに情報を流出させることができる。

一部のティックusbの変型では、USBメモリで拡張子がEXEの実行ファイルを探して改ざんする。改ざんされたEXEファイルはエントリポイントが修正され、特定コードを実行するようになり、ファイル末尾に追加された実行ファイルを実行させる。

4.セキュリティUSBメモリの攻撃

韓国国内企業の内部情報流出を目的としたティックusbの攻撃の場合、企業で使用されているセキュリティUSBメモリを感染させ、これをマルウェアの拡散経路として利用する方式を使用した点から推測して、彼らは韓国国内のIT環境およびインフラをすでに相当な水準で把握しているものと思われる。

2012年から2014年の間に発見された一部のティックusbは、韓国国内企業の特定のセキュリティUSBメモリが接続されている場合、そのUSBドライブの特定領域からデータを読み取り実行することが確認された。このセキュリティUSBメモリにどのようなコードが含まれているかはわからないが、攻撃者はUSBメモリの製造段階で悪意のあるコードを組み込んだ可能性もある。このような攻撃方法は、ネットワークから分離した企業システムを攻撃するための目的があると推定される。

5.難読化

スクリプトで作成されたマルウェアは、分析や診断を難しくするためにコードの一部或いは大半を難読化させる。2009年に発見されたソロウ(Solow)の変型は、一部の文字列を暗号化していた。2010年以降にスクリプトで製作されたマルウェアでは、ほとんどのコードが難読化されている。

6.自己保護

複数のプロセスを実行して互いに実行の有無を確認し、もし一つのプロセスが終了しても、再度実行してユーザーによるマルウェアの除去を困難にす

る。一部のマルウェアは、ユーザーモード隠蔽機能を含む場合もある。ユーザーによる発見を困難にするために、分析ツール、レジストリエディタ、システム構成プログラム等を実行できないようにすることもある。

最近の韓国国内における活動の事例

2018年以降、アンラボにおいて収集されたUSBフラッシュメモリを利用して拡散するマルウェアは、次の通りである。

日時	収集場所	内容	ファイル名およびMD5
2018年3月	医療	2016年7月発見。JS/Bondat。自己防御技法を使用するマイナー(Miner)	a81b4d4971f2fcb739b384e33e6053e6 (http://asec.ahnlab.com/1099)
2018年7～8月、 2019年4月	製造、 電子、金融	2009年発見サンプル。複数業種において発見。Thumb.dbファイル。宗教関連内容のプリント	0a456ffff1d3fd522457c187ebcf41e4、 977a2c8088b38e086137938079b25f43
2018年12月	重工業	LNK/Retadup.AutoHotKeyで作成されたスクリプト。LNKファイル作成	328c03ca3c396c9c29518498a41b74ac (実行のたびに内容が異なり、ハッシュが異なる)
2019年7月	金融	2015年発見。IrcbotでautorunおよびLNKファイルを作成	winmgr.exe : 5c7a77c4ecbdb0a4b234b8d10f5a0c81
2019年9月	流通	飲食売場のPOSで疑いのあるトラフィックを発見。調査の結果、2018年4月に感染し、ルートキット機能により感染状態での診断/治療が困難	ランダムファイル名.exe a23f2799d70decce3fa37db9a7c0a9d1 d027b6120806146d04d20585b612fe6b
2019年9月	製造	2010年に発見されたAutorun、Palevo等、多数のマルウェア	e1e3845ebb46f7afa05b9b80fd21aef6 a92ac88d8a5dfd2a9dffc5608ce65ab4 9fd7b8adb27381bd2a4d6e51324ca63c 164e1aab8107acb9aede9e2424012c13 45bc780a1a31c3baac135ac9563f010a cf1354bf2fb650b26bbe3dd2130f9a0b
2019年10月	教育	元のファイルのFILESフォルダに保存後、正常なものと同じLNKファイルを作成。Files.bat作成	4ffd2baf81e34ed4dfe0471f55b346ee
2019年10月	IT	2006年に発見された難読化されていない初期VBS/Solowの変型	2d5e9f0af1e78f0078c68bf1a35ccb1e
2019年12月	企業	Autoitで作成されたスクリプトを実行するLNK	729857a300e3e3cb76a4850a2b66d525
2020年2月	製造	Bflientの変型	cb9b8d4943e85553dfd9a1aee7d1878f
2020年2月	IT	Bflientの変型	18f3a44388176725ab179cac6309fd46

2020年5月	教育	リムーバブルディスクにRECYCLフォルダとrknl.vbsファイルを作成。LNKファイル。Minerダウンロード。Officeドキュメントの感染	8f52324624698d2dec6244e010b33a52 822032d5d49dc1daed3d819c87b07cc6
2020年6月	流通	2010年に発見されたワーム。リムーバブルディスクのフォルダ内に、フォルダ名と同じファイル名のファイルを作成し、フォルダと誤認させて実行を誘導	c027aeac082f01c7a6c194b04c410383

[表2] USBメモリ関連マルウェアの韓国国内における感染事例

2018年~2020年に活動が報告されたマルウェアを通して、10年前に発見されたマルウェアがいまだに活動していることがわかる。

これらは新しいマルウェアではなく、ほとんどが従来のアンチウイルスプログラムで問題なく診断/治療(削除)が可能な場合がほとんどだが、アンチウイルスプログラムのインストールが困難な低仕様のシステム、安定性を理由にプログラムのインストールが制限されるメーカーの生産設備、POS(Point of Sales)システム等がほとんどである。従って、実際のマルウェア感染被害はさらに大きいものと考えられる。

USBメモリ内のファイルをLNKファイルと交換する攻撃方法は、現在でも有効な攻撃方法である。2019年、売場のPOSシステムにおいて異常パケットが捕捉され、確認した結果マルウェアが発見された。このシステムは、2018年にメンテナンスのために接続したUSBメモリ内のLNKファイルをシステム設定変更ファイルと勘違いしてマルウェア(md5: a23f2799d70decce3fa37db9a7c0a9d1)に感染したものであり、他のシステムではPalevoワーム(md5: d027b6120806146d04d20585b612fe6b)が発見された。

生産設備システムやPOSシステムのように特殊な目的で使用されるシステムは10年以上運用されることもあり、マルウェアに感染した状態のままで数年間運用されることもある。

対応および予防

AhnLab V3プロダクトラインで「CD/USBドライブの自動実行防止」機能と「USBドライブの自動チェック」機能を有効にすると、USBメモリが接続されたときに自動実行を防止し、既知のマルウェアを診断できる。

USBメモリを通して拡散するマルウェアは、製造産業分野で持続的に感染が報告されている。多くの企業において、セキュリティポリシー上、生産工程内部へUSBメモリを持ち込むときはアンチウイルスプログラムで検査する必要があるが、実際にはこのような手順を無視して生産設備がマルウェアに感染する事例が頻繁に報告されている。

生産設備や特殊目的システムは、これまで外部とのインターネット接続が行われていなかったために相対的にセキュリティが疎かになっていたが、ランサムウェア攻撃により生産工程やサービスが中断される事例が発生し、外部にセキュリティ上の問題が知られるようになった。しかし、生産設備や特殊目的システムにおいて、マルウェアがUSBメモリを通して拡散する被害は、10年以上前から報告されていた。USBメモリを通してマルウェアが拡散する技法は古くから存在し、これらのシステムを対象とはしておらず、アンチウイルスプログラムでも容易に検出され、新種でもないため、大し

た問題ではないと考えられる。しかし、攻撃者が特定の産業やサービスを対象としてマルウェアを製作するならば、深刻な問題が発生することがある。

アンチウイルスプログラムで診断可能であり、旧型のシステムでのみスムーズに動作するこれらのマルウェアが、10年以上、特定の産業において盛んに活動しているという点について、いくつかの教訓を得ることができる。依然として多くの人々がアンチウイルスプログラムのインストールのような最低限のセキュリティを遂行しておらず、内部に持ち込まれた記憶メディアに対するセキュリティポリシーが遵守されていないという点である。内部システムがUSBフラッシュメモリを通してマルウェアに感染する前に、それを防ぐことができる様々な機会がある。1つ目に、メンテナンス担当者のコンピュータがマルウェアに感染していない場合、USBメモリがマルウェアに汚染されなかった。ほとんどは新種のマルウェアではないため、アンチウイルスプログラムさえインストールしていれば、感染を防ぐことができる。2つ目に、メンテナンス担当者が持参したUSBメモリを内部に持ち込むときに、アンチウイルスプログラムでチェックを行えば、内部への流入を防ぐことができる。3つ目に、システムにアンチウイルスプログラムやホワイトリストベースのセキュリティプログラムがインストールされていれば、マルウェアに感染することはない。

新たなセキュリティの脅威に対する備えも重要だが、すでに関連するセキュリティパッチも出ており、アンチウイルスプログラムでの診断/治療も可能であり、定められたセキュリティポリシーさえ遵守すれば被害を減らすことができる過去のマルウェアに対する対策のほうが、より容易ではないかと思われる。

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)