AhnLab

安全月刊

2020.08 Vol.93

USB 恶意代码趋势分析报告

USB闪存驱动器恶意代码趋势分析报告

在 USB 闪存驱动器上存活 10 年的恶意代码

从事安全业务相关工作的人们通常会对新的安全威胁的动向和响应方案感兴趣。但是，10年前出现的通过USB(Universal Serial Bus)闪存驱动器传播的恶意代码的破坏仍在发生。该报告分析了过去三年中报告的通过USB闪存驱动器传播恶意代码的变化和特点以及在韩国的活动。

USB闪存驱动器是一种用于存储信息的设备，在中国一般被称为U盘。USB闪存已经成为目前使用最广泛的可移动存储设备。与传统的移动存储产品软盘相比， 它的容量大、体积小、方便携带， 但由于发生了内部数据泄漏等问题， 有些企业和机构限制了USB闪存的使用。然而， USB闪存的使用限制导致了用户的不便， 很难适用于所有系统。因此，一些机构和企业在操作系统上应用了例外策略。

在以下特定领域，通过USB闪存驱动器传播的恶意代码持续造成损害。

- 制造业（低配置或旧版本系统）
- 专用系统（ATM、POS系统、信息亭）
- 公用系统（学校、图书馆等）
- 安全策略例外系统等

在制造业领域，如果在生产过程中没有发生问题，则仍将使用已停止服务支持的诸如Windows XP之类的操作系统（OS）。据霍尼韦尔（HoneyWell）介绍，USB闪存驱动器是在运营技术（Operation Technology, OT）系统中第二被广泛使用的工业矢量漏洞。在工业界和诸如ATM、POS系统和信息亭等专用系统也在使用低配置的旧版本操作系统。

在这些领域中，在将系统与存储维护程序或数据文件的USB闪存驱动器连接的过程中，会发生恶意代码的感染的情况。尽管在韩国的医院中没有太多有关恶意代码感染的报告，但由于医疗设备也可能使用旧版本的操作系统，因此需要格外注意。在这些系统中，有很多都设有安装安全程序，并且这些系统可能在受感染的状态下运行长达几年。

与 USB 闪存驱动器相关的恶意代码的进化

利用可移动存储设备的攻击始于20世纪80年代。在20世纪80年代和90年代初期，系统主要通过软盘启动，因此软盘是病毒传播的主要途径。虽然有人可能会提出当今时代是否还会使用软盘的疑问，但直到2019年，通过软盘运营运行核武器管理系统。随着硬盘的普及，使用软盘启动的情况逐渐减少，并随着Windows时代的到来，启动型病毒开始急剧减少。

随着20世纪90年代中期 CD-ROM的大众化，操作系统也添加了一个功能，即是当用户将存储介质插入到系统时自动运行指定文件。但是，攻击者也随之开始使用了自动运行功能。1998年4月，利用QuickTime 2.0和自动运行（AutoPlay）功能传播的AutoStart蠕虫病毒在Mac开始扩散。2005年10月，发生了索尼BMG唱片中包含Windows Rootkit的事件，该事件也与CD-ROM媒体的自动运行功能有关。

随着2000年USB闪存驱动器的推出，它们取代了软盘和其他可移动存储介质。可以读写的新的可移动存储介质的扩散和自动运行功能对恶意代码制作者来说是一个全新的机会。2006年，出现了一种蠕虫，该蠕虫会在USB闪存驱动器中生成Autorun.inf文件，并在将USB闪存驱动器连接到计算机时会自动运行恶意代码，并从2007年开始逐渐成为一种问题。

与主要USB闪存驱动器相关的恶意代码的进化如下：

时间	内容
2006年	出现利用自动运行（Autorun）功能传播的Solow等蠕虫病毒
2008年	在安全会议上分发的USB闪存驱动器中发现了恶意代码
2008年11月	美军公开了遭受Agent.BTZ恶意代码攻击的事件
2008年12月	发现通过SMB漏洞和USB闪存驱动器传播的Conficker蠕虫病毒
2009年	出现代码混淆脚本型蠕虫病毒
2009年	发现数据泄露型自动运行（Autorun），在韩国发现的变种还收集HWP文件

2009年7月	推出Winows 7，自动运行不可用
2010年	发现震网病毒（Stuxnet）
2011年	在针对性攻击中利用USB闪存驱动器传播
2013年	在USB闪存驱动器中创建文件名的快捷方式（LNK）文件的蠕虫病毒扩散
2014年	出现感染USB闪存驱动器的可执行文件后攻击内部系统的Tickusb活动
2014年	发现具有通过USB闪存驱动器传播和键盘记录功能的Dotlogger
2016年	出现将USB闪存驱动器中的文件和文件夹移动到特定文件夹，并生成同名LNK文件的蠕虫病毒
2020年	发现利用USB闪存驱动器传播或收集USB闪存驱动器中信息的USBferry、Ramsay、Compfun、USBCulprit恶意代码

[表1] 通过USB闪存驱动器传播的恶意代码的进化

Solow（发现于2006年）是一种用Visual Basic Script(VBS)编写的脚本蠕虫，首次被发现时没有任何代码混淆。该蠕虫的字符串没有代码混淆，并发现了多样的变种，例如仅生成文件名略有不同或添加注释的变种，或者在复制文件过程中修改部分代码等。

生成Autorun.inf文件并将其传播的恶意代码自2007年开始出现了多样的种类，并广泛扩散。2008年和2010年，在安全会议上分发的USB闪存驱动器上发现了恶意代码，在国际空间站（ISS）计算机上也发现了恶意代码。

2008年11月， 美军发现了Agent.BTZ蠕虫病毒。该恶意代码在2011年也仍然是一个问题。众所周知， 该恶意代码是Turla组织的恶意代码，推测Turla组织受特定国家/地区的支援。2020年5月，在韩国也发现了该恶意代码的最新版本4的变种。

2008年12月发现的Conficker蠕虫病毒变种的利用其早期版本的利用CVE-2008-4250(MS08-067)漏洞传播功能，并使用自动运行功能通过USB闪存驱动器传播。Conficker蠕虫病毒是目前在业界最常见的恶意代码，它利用MS08-067漏洞感染其他连接的系统。即使发现了漏洞并发布了安全补丁， 但仍有一些系统已有10年以上未进行安全更新，因此发生上述的利用漏洞感染系统的问题。

最初 ， 它只是在传播 ， 但部分蠕虫病毒包含了数据泄露功能。2009年发现的Autorun蠕虫病毒 （ md5: d81569c475154ddf7ab32ce7af393866 ） 是针对韩国用户传播的。该恶意代码在系统中收集包括韩文文件（HWP）的多个文档文件。该变种生成的自动运行（autorun.inf）文件中包含韩文，例如“打开文件夹以查看文件”、“打开”，因此，估计该文件是针对韩国用户制作的。

2010年发现的震网病毒（Stuxnet）利用USB闪存驱动器的漏洞进行传播。利用LNK漏洞（CVE-2010-2568），只需通过Windows资源管理器打开快捷方式文件所在的目录， 即可自动运行快捷方式文件。在韩国， 2011年发生了利用LNK漏洞传播恶意代码的针对性攻击。

USB闪存驱动器在网分离或网闸 （air-gap） 系统中用于复制数据。攻击者制作了一个恶意代码， 该代码泄露USB闪存驱动器中保存的重要数据 。自2010年以来， 攻击者就一直尝试通过这种方式进行攻击。2010年， 在韩国还发现了一种在感染恶意代码的状态下连接USB闪存驱动器时 ， 将压缩USB闪存驱动器中的文件并将其传送到网络的恶意代码。

从2009年推出的Windows 7开始，除了CD-ROM之外的所有驱动器类型都禁用自动运行。随着新的Windows操作系统的普及，利用autorun.inf文件的自动运行功能不再可用，恶意代码制作者则利用快捷方式（LNK）文件创建蠕虫病毒，而不是利用autorun.inf文件。而在2013年后，这一攻击方法已经十分普遍。这些恶意代码会继续进化，不仅会创建LNK文件，还会将USB闪存驱动器中的文件和文件夹移动到“.Trashes”文件夹，并用与文件和文件夹相同名称的快捷方式文件替换它们（md5: 3f097745bc355e14961023392e369ed9）。该恶意代码更改系统设置， 使隐藏文件不可见， 并将 “.Trashes” 文件夹属性设为隐藏， 以便无法在资源管理器中查看它。

2014年1月， 在未连接互联网的地区也发现了通过USB闪存驱动器传播的恶意代码。由于没有物理连接互联网，因此， 每周一次， USB闪存驱动器用于保存防病毒软件的补丁文件或引擎文件等维护所需文件， 而在这一使用过程中发现了上述的恶意代码。

2014年， Tick组织的Tickusb是利用USB闪存驱动器以泄露韩国企业机密信息等为目的制作的恶意代码， 并确认了其从2014年春季至2017年11月的活动。当运行恶意DLL文件时，它将在特定路径上生成日志文件，并检查USB闪存驱动器的连接状态。如果USB闪存驱动器已连接系统， 则运行恶意EXE文件， 并下载其他文件。恶意EXE文件根据其变种执行的功能略有不同 ， 但是通常会收集USB闪存驱动器中文件的信息。有些变种还会篡改USB闪存驱动器中的EXE文件。如果将带有最终篡改的EXE文件的USB闪存驱动器连接到另一个系统， 然后运行该文件， 则计算机也感染了Tickusb。2015年4月， 发现了Tickusb的变种Cryptbase.dll。与其他Tickusb变种不同的是， 它是一个独立的DLL文件。它具有与Windows正常CRYPTBASE.dll文件相同的导出函数， 并且发现的文件路径为：%ProgramFiles%\common files\java\java update\cryptbase.dll。据此，可以推测恶意代码是在运行与Java相关程序时加载的。

在2015年6月1日发生的攻击中，发现了由DLL文件和EXE文件构成的变种。攻击者修补了兄弟（Brother）打印机驱动程序文件BrSrMonW.exe安装， 以在运行该文件时加载恶意DLL文件BrWeb.dll。EXE文件具有在USB闪存驱动器中查找并篡改EXE文件的功能。2016年10月 ， 发现了Tickusb的变种wincrypt.dll(md5: 16572393021beea366679e80cc78610c)，直到2017年11月为止，仍然可以确认具有相同文件名的变种。

从2014年6月开始，发现了用 “.NET” 编写并通过autorun.inf文件传播的Dotlogger。该恶意代码同时具有键盘记录器功能，并且于2017年发现的变种（md5: 664b3007c043c26cff911d8b400bd0bf）具有禁用防病毒软件程序的功能。在2016年之后发现的蠕虫病毒还会下载并运行挖掘加密货币的挖矿（CoinMiner）恶意软件。

2020年，趋势科技（Trend Micro）公开了USBferry，ESET公开了Ramsay，卡巴斯基（Kaspersky）公开了Compfun和USBCulprit等恶意代码信息，这些恶意代码会窃取USB闪存驱动器中的数据，或通过USB闪存驱动器攻击网络分离系统。

恶意代码利用 USB 闪存驱动器的技术和手法

攻击者使用各种方法来传播恶意代码以保护自己。

1.传播 - 生成autorun.inf

从Windows 95开始，当CD-ROM或USB闪存驱动器连接到计算机时，将自动运行autorun.inf文件指定的特定文件。攻击者利用该功能在可移动磁盘上创建自动运行文件，导致恶意代码自动运行。

2006年（也可能是2005年以前）首次发现了在可移动磁盘上创建自动运行文件并运行特定文件的恶意代码，并在USB闪存驱动器、存储卡和移动硬盘等可移动存储设备上生成自动运行文件。通过将垃圾直添加到自动运行文件中以妨碍诊断。但在Windows 7之后，它将不再用以这种方法自动运行。

2.传播 - 诱导运行

在Windows 7之后的操作系统中，使用autorun.inf文件的自动运行功能不再可用，并且攻击者创建现有文件的快捷方式（Shortcut）文件或创建图标形状与文件夹相同的文件，以诱导用户点击。可移动磁盘中存在的文件夹或文件，或者文件夹和文件都被更改为隐藏属性，并生成与文件夹或文件同名的快捷方式LNK文件。用户会误认为快捷方式文件就是原本存在于USB闪存驱动器中的文件并点击。一些恶意代码会更改注册表内容，将“快捷方式”图标中的箭头删除，从而使用户很难判断其是否为快捷方式。

3.传播 - 感染USB闪存驱动器中可执行文件

在网分离系统中，也会使用USB闪存驱动器来复制文件。一些恶意代码试图篡改USB闪存驱动器中可执行文件来入侵内部系统。攻击者利用恶意代码感染连接互联网的系统，并在连接USB闪存驱动器时感染USB闪存驱动器中的EXE文件。

在与外部断开连接的系统中使用USB闪存驱动器并运行恶意代码时，会在USB闪存驱动器中收集和存储信息，并且在连接互联网的系统中使用USB闪存驱动器时，信息可能会泄漏。

一些Tickusb变种会在USB闪存驱动器中找到并篡改扩展名为EXE的可执行文件。篡改后的EXE文件的入口点被更改并运行特定代码，然后运行添加到文件末尾的可执行文件。

4.攻击安全的 USB闪存驱动器

以泄露韩国企业内部信息为目的的Tickusb攻击，感染企业使用的安全USB闪存驱动器，并将其利用为传播恶意代码的途径。从这一点可以看出，攻击者似乎已经相当程度地掌握了韩国IT环境及基础设施。

在2012年至2014年之间发现的一些Tickusb，已确认当连接韩国企业的特定安全USB闪存驱动器时，可以读取

和运行该USB闪存驱动器特定区域的数据。虽然无法获知相关安全USB闪存驱动器中包含何种代码 ， 但攻击者可能已在USB闪存驱动器制造阶段就注入了恶意代码。估计这种攻击方式是为了攻击网络分离的企业系统。

5.代码混淆

使用脚本编写的恶意代码会混淆部分或大部分代码 ， 从而使分析或诊断变得困难。2009年发现的Solow变种对一些字符串进行了加密。自2010年以来，使用脚本编写的恶意代码大部分都是经过代码混淆的。

6.自我保护

运行多个进程，以相互确认是否正在运行，如果一个进程结束，则将重新运行，从而使用户很难清除恶意代码。一些恶意代码还包含了用户模式隐藏功能。为了使用户难以发现 ， 有时会禁用分析工具、注册表编辑器、系统配置程序。

近期在韩国的活动事例

自2018年以来，AhnLab收集的通过USB闪存驱动器传播的恶意代码如下：

时间	收集处	内容	文件名及MD5
2018年3月	医疗行业	2016年7月发现 JS/Bondat 使用自我防御手法的挖矿恶意代码 （Miner）	a81b4d4971f2fcb739b384e33e6053e6 (http://asec.ahnlab.com/1099)
2018年7~8月， 2019年4月	制造 电子 金融	2009年发现样本 被多家企业发现 Thumb.db文件 与宗教有关的内容印刷品	0a456ffff1d3fd522457c187ebcf41e4, 977a2c8088b38e086137938079b25f43
2018年12月	重工业	LNK/Retadup 用AutoHotKey编写的脚本 生成LNK文件	328c03ca3c396c9c29518498a41b74ac （因每次运行时的内容都有所不同，故哈希也不同）
2019年7月	金融	2015年发现 用Ircbot生成autorun.inf及LNK文件	winmgr.exe : 5c7a77c4ecbdb0a4b234b8d10f5a0c81
2019年9月	流通	在餐饮卖场POS机上发现可疑流量 调查结果显示，在2018年4月遭到感染，在以Rootkit功能感染的状态下很难诊断和治疗	随机文件名.exe a23f2799d70decce3fa37db9a7c0a9d1 d027b6120806146d04d20585b612fe6b
2019年9月	制造	2010年发现的Autorun和Palevo等多种恶意代码	e1e3845ebb46f7afa05b9b80fd21aef6 a92ac88d8a5dfd2a9dffc5608ce65ab4 9fd7b8adb27381bd2a4d6e51324ca63c

			164e1aab8107acb9aede9e2424012c13 45bc780a1a31c3baac135ac9563f010a cf1354bf2fb650b26bbe3dd2130f9a0b
2019年10月	教育	将原始文件保存到FILES文件夹中， 然后生成与正常文件相同的LNK文件 生成Files.bat	4ffd2baf81e34ed4dfe0471f55b346ee
2019年10月	IT	2006年发现的未进行代码混淆的初期VBS/Solow变种	2d5e9f0af1e78f0078c68bf1a35ccb1e
2019年12月	企业	运行用Autoit编写的脚本的LNK	729857a300e3e3cb76a4850a2b66d525
2020年2月	制造	Bflient变种	cb9b8d4943e85553dfd9a1aee7d1878f
2020年2月	IT	Bflient变种	18f3a44388176725ab179cac6309fd46
2020年5月	教育	在可移动磁盘上生成RECYCL文件夹和rknl.vbs文件 LNK文件 下载挖矿恶意代码感染办公文档	8f52324624698d2dec6244e010b33a52 822032d5d49dc1daed3d819c87b07cc6
2020年6月	流通	2010年发现的蠕虫病毒 在可移动硬盘内的文件夹中生成与文件夹名称相同的文件， 并诱导用户误认为其为正常文件夹而运行	c027aeac082f01c7a6c194b04c410383

[表2] 韩国有关通过USB闪存驱动器感染恶意代码的事例

通过2018年至2020年期间报告活动的恶意代码，可以看出10年前发现的恶意代码至今仍然在活动。

这些不是新的恶意代码，其中大多数可以通过现有的防病毒程序是诊断和治疗（删除）。但是，由很多系统是难以安装防病毒程序的低配置系统 ， 或由于稳定性而限制了防病毒程序的安装的制造商的生产设备以及POS(Point of Sales)系统。因此，可以说恶意代码感染的实际损失更大。

用LNK文件替换USB闪存驱动器中文件的攻击方式仍然是有效的攻击方式。2019年， 在商场的POS系统中发现了异常的数据包， 经过确认后发现是恶意代码。由于将连接的USB闪存驱动器中的LNK文件误认为是系统设置更改文件，从而感染了恶意代码（md5: a23f2799d70decce3fa37db9a7c0a9d1），在其他系统中则发现了Palevo蠕虫病毒（md5: d027b6120806146d04d20585b612fe6b）。

专用系统（例如生产设备系统和POS系统）可以运行10年以上，而且在感染恶意代码的情况下，也依然会运行数年。

响应及预防

在AhnLab V3产品系列中，通过启用“防止CD/USB驱动器自动运行”功能和“自动扫描USB驱动器”功能，可以在连接USB闪存驱动器时防止自动运行，并诊断已知的恶意代码。

在制造业领域， 不断报告通过USB闪存驱动器传播的恶意代码。很多企业的安全策略要求在将USB闪存驱动器带入生产工艺时，对其进行防病毒程序扫描，但实际上，由于通常都会忽略此过程，从而导致生产设备经常被恶意代码感染。

此前，生产设备或专用系统由于未连接互联网，因此相对疏忽了安全防护工作。但是，生产设备和专用系统通过USB闪存驱动器传播的恶意代码遭都破坏的报告已有10年以上。通过USB闪存驱动器传播恶意代码的方法已经很老旧，并未针对这些系统，而且通过防病毒程序也能诊断，因此很容易将其视为无关紧要的问题。但是，如果攻击者以特定产业或服务为目标制作恶意代码的话，后果可能不堪设想。

这些恶意代码可以通过防病毒程序诊断出来，并且只能在旧系统上正常运行，以及在特定产业活跃了10年。从这些事实中我们可以吸取教训。尽管如此， 仍然有很多人没有采取诸如安装防病毒程序等的最低限度的安全措施， 而且流入内部的储存设备也未遵守安全策略。有很多机会可以防止内部系统在通过USB闪存驱动器闪存感染恶意代码 。首先，除非维护人员的计算机感染了恶意代码，否则USB闪存驱动器不会被恶意代码感染。因为大部分都不是新型的恶意代码，所以只要安装了防病毒程序，就可以防止感染。其次，如果将维护人员的USB闪存驱动器带入内部时，通过防病毒程序进行检查，可以防止其流入内部。第三，如果系统安装了防病毒程序或基于白名单的安全程序，则可能不会感染恶意代码。

应对新的安全威胁固然重要，但应对已知恶意代码也很重要。因为，已知恶意代码的相关安全补丁已经可用，而且还可以通过防病毒程序进行诊断或治疗，因此，只要遵守建立的安全策略，可以减少损失。

AhnLab

安全月刊

https:// cn.ahnlab.com

https://global.ahnlab.com

https://www.ahnlab.com

关于AhnLab

Ahnlab的尖端技术和服务不断满足当今世界日新月异的安全需求，
确保我们客户的业务连续性，并致力于为所有客户打造一个安全的计算环境。
我们提供全方位的安全阵容，包括经过证实的适用于桌面和服务器的世界级防病毒产品、
移动安全产品、网上交易安全产品、网络安全设备以及咨询服务。
AhnLab已经牢固地确立了其市场地位，其销售伙伴遍布全球许多国家和地区。

AhnLab

北京市朝阳区望京阜通东大街1号望京SOHO塔2 B座 220502室 | 上海市闵行区万源路2158号18幢泓毅大厦1201室
电话：+86 10 8260 0932（北京） / +86 21 6095 6780（上海） | cn.sales@ahnlab.com