AhnLab

安全月刊

2022.05 Vol.114

恶意 Word 文档类型分析报告

利用 Word 文档传播恶意代码之攻击方式的变化

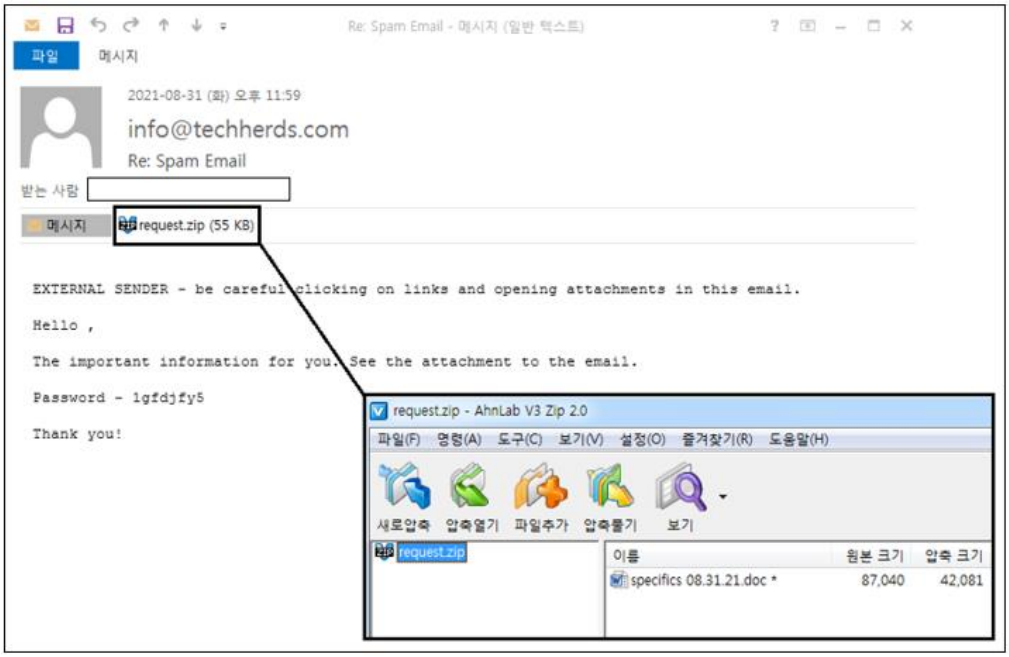
利用恶意Word文档的攻击一直以来都不断被发现。它利用了Word文档是用户最常用的文件格式这一事实。攻击者主要通过钓鱼邮件传播恶意Word文件，并根据目标而改变内容或升级传播方式等，使用更加复杂的方法发动攻击。

在本文中，我们将对2021年至2022年初传播最活跃的恶意Word文档类型及运行过程的变化进行重点分析。

利用恶意Word文档的攻击将恶意代码分发到用户的系统中，以执行窃取信息等恶意行为。此时分发的恶意代码呈现出非常多样化的传播和变化方式。从2021年至2022年初，传播最活跃的恶意Word文档是TA551（Shathak）攻击组织使用的Word文档类型。虽然该类型并非是最近发现的，但值得注意的是，在2020年，通过同一类型的Word文档仅传播IcedID恶意代码，而从2021年起，开始传播IcedID、Qakbot、Trickbot和BazarLoader等各种类型的恶意代码。下面我们将对TA551攻击组织使用的Word文档类型（以下简称“TA551类型”）的主要特征进行分析。

TA551 类型恶意 Word 文档的传播方式

大部分恶意Word文件作为针对企业用户的钓鱼邮件的附件传播。针对特定用户，攻击者会利用包含与用户相关内容的文本或Word文件，而针对非特定人群，会利用包含订单、报价单等一般内容的恶意Word文档。其中TA551攻击组织所使用的方式是后者。对伪装成订单的Word文档进行加密并以压缩文件形式附加到邮件，邮件正文中包含了诱导用户打开附件的内容（参见【图1】）。



【图1】附加恶意Word文档的钓鱼邮件

2021年6月以后，大量传播的TA551类型的Word文档不断变种传播。其变形的重点包括宏代码的样式变化，最终恶意代码下载进程的增加，最终恶意代码变种等。不过，在这些变形过程中，文档文件名和文件内容格式并无显著变化，具有较高的相似性。

【表1】列举了在2021年间传播的TA551恶意Word文件名中的一部分。TA551类型的Word文档运行方式是，在运行宏指令后，释放（Drop）HTA文件，其后下载附加恶意代码，因此列举了这三种文件的文件名。

Attached File (*.doc)	Dropped HTA	Downloaded Malware
deed contract_06.21.doc	winSelBefore.hta	winSelBefore.jpg
charge, 06.28.2021.doc	dCurTable.hta	dCurTable.jpg
decree.06.28.2021.doc	doubleBorderInt.hta	doubleBorderInt.jpg
report-06.21.doc	repoRequestDocument.hta	repoRequestDocument.jpg
facts,06.21.doc	objectVarQuery.hta	objectVarQuery.jpg

report-09.21.doc	1.hta	docExObj.jpg
ordain_09.21.doc		divDocDev.jpg
direct 09.21.doc		winObj.jpg
adjure 09.21.doc		objWinDoc.jpg
commerce .08.21.doc		dirDirDrive.jpg
document-08.30.2021.doc		winEx.jpg
commerce -08.21.doc		devDevDiv.jpg
deed contract,09.21.doc		docDirObj.jpg
deed contract-09.21.doc		devDirWin.jpg

【表1】传播文件名（部分）

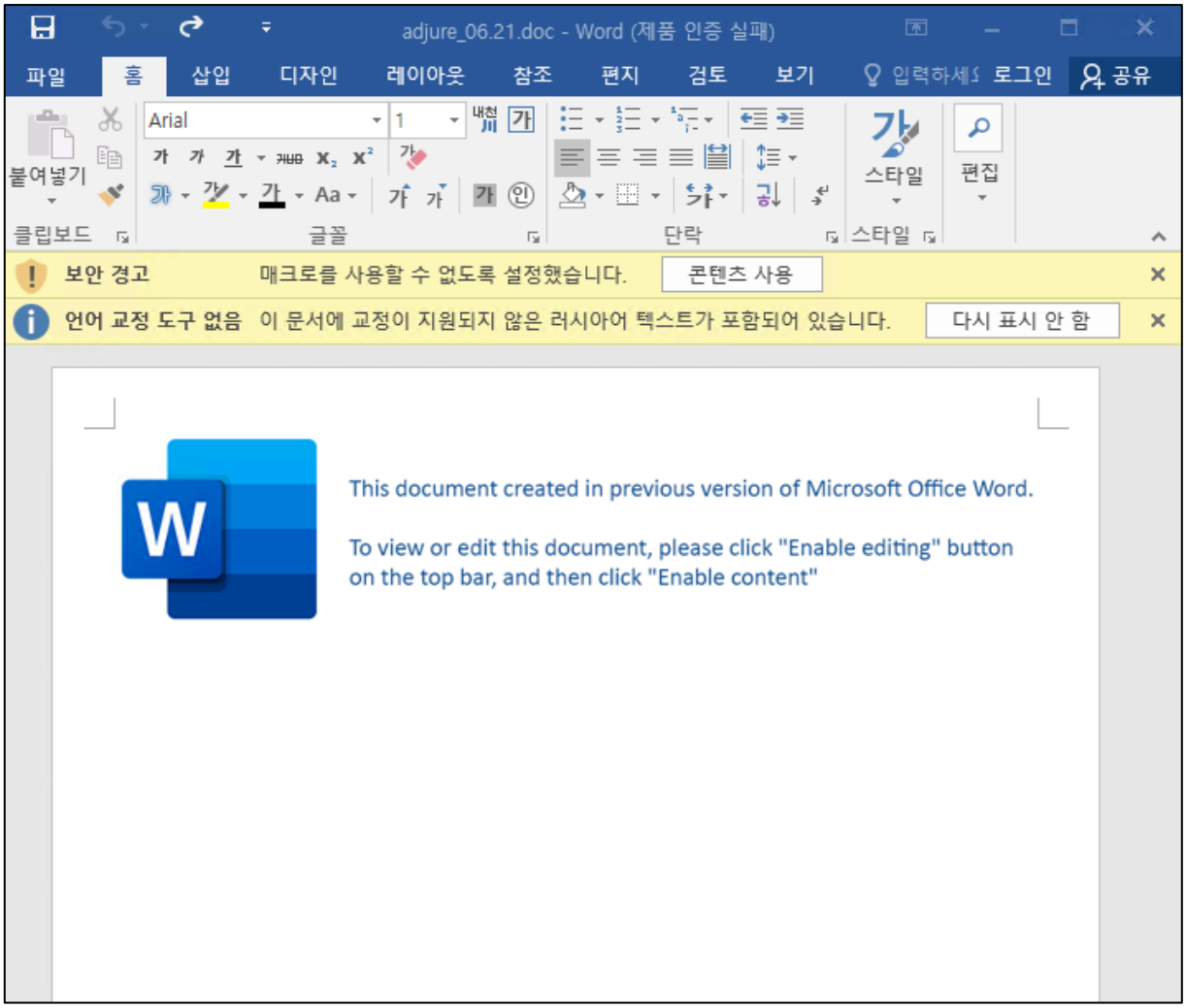
运行方式及特征

恶意Word文件的整体运行过程参见【图2】

【图2】恶意Word文件运行过程

钓鱼邮件附件中的恶意Word文件，会在恶意VBA宏指令内部的宏指令运行的过程中，生成HTA(HTML Application)文件。并利用Word正文区域设置成白色与1pt大小的文字将HTA文件的数据隐藏起来。运行HTA文件后，会通过外部URL下载其他的恶意代码。

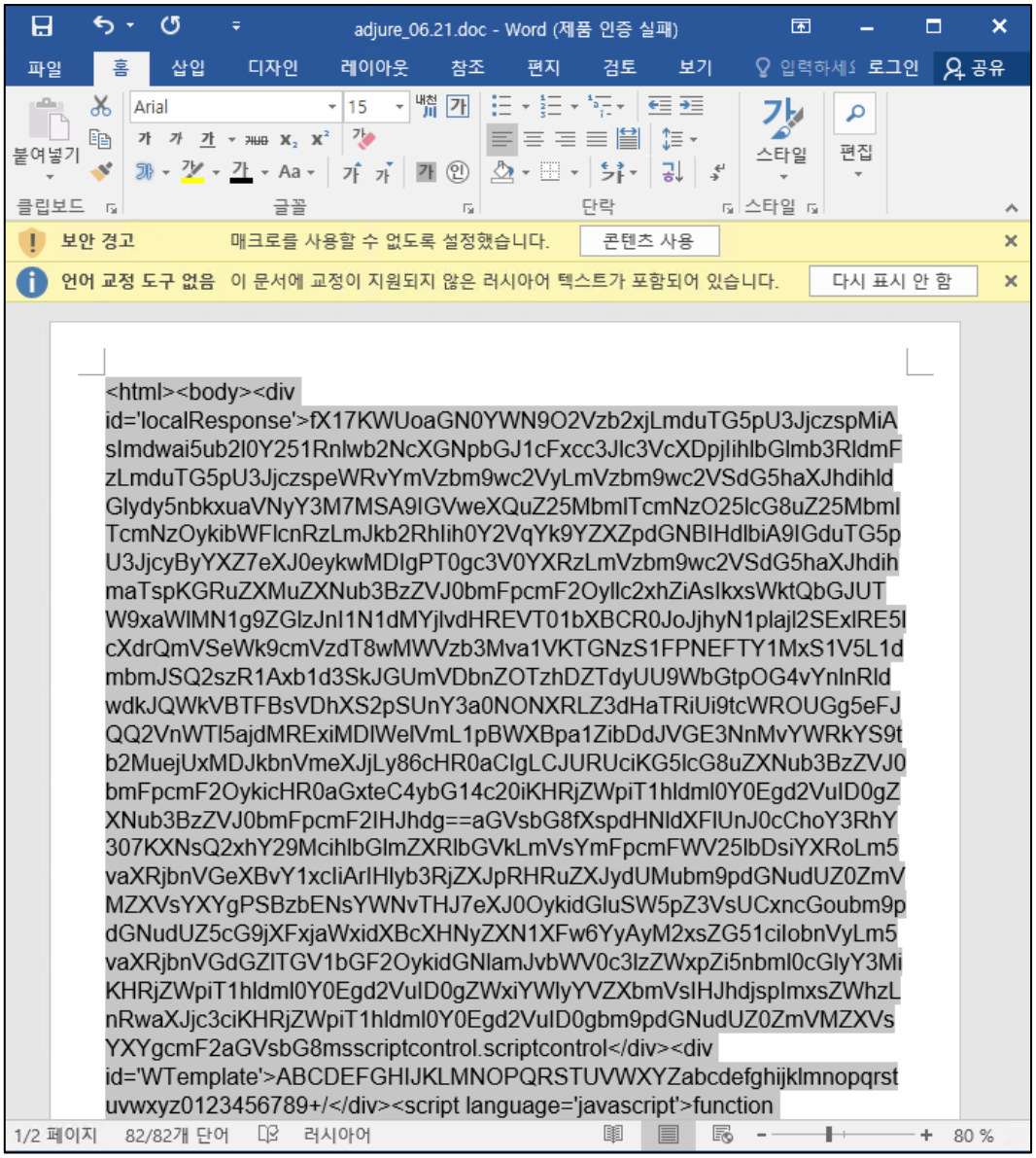
由于HTA文件不受网络浏览器安全策略的影响，它们可以运行不受信任的程序，还可以使用PowerShell，因此经常被攻击者恶意使用。



【图3】TA551类型的Word文件正文

TA551类型Word文件的主要特征如【图3】所示，单独插入了诱导开启宏指令的图片。从2020年起发现的TA551类型Word文件大部分都使用了类似的图片。

如果删除诱导开启宏的图片文件，可以看到设置为白色字体的隐藏数据。如果改变字体的属性，则会显示HTML源代码，如【图4】所示。该数据成为Word文档运行宏时下载至本地路径的HTA文件的内容。



【图4】恶意Word文件中隐藏的HTML源代码

宏代码运行时会基于整个文档的内容创建一个HTA文件，然后explorer.exe通过mshta.exe运行该HTA文件。

【图5】RAPIT（恶意代码自动分析基础架构）进程树

如果查看AhnLab RAPIT基础架构中进程树（Process Tree），可以看到由mshta.exe进程运行HTA文件，并随即下载jpg扩展名文件，而后加载到rundll32.exe并运行。实际上，从运行HTA脚本后链接的URL下载DLL执行文件（Portable Executable），但确认到在其过程中并没有直接使用.dll扩展名，而是使用了jpg扩展名。

可以推断这是为了下载执行文件的过程中，逃避对可疑行为的拦截，而这种方式是TA551类型Word文档文件中常用的手法。

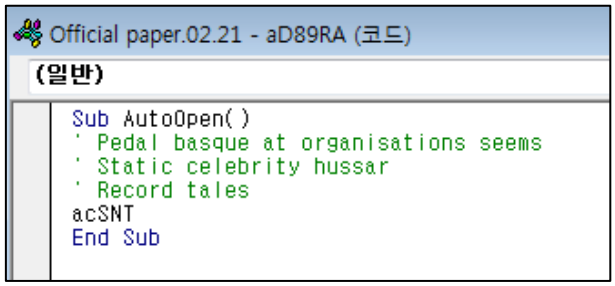
运行方式的变化

前文中所介绍的恶意Word文档运行过程中，其整体框架是不变的。但是，可以看到在宏运行过程中会发生两种变形。即“VBA宏代码及HTA文件的变种”及“传播阶段的扩张所引起的最终恶意代码种类的变化”。

其中，VBA宏代码的样式变形频繁发生。我们发现存在HTA文件的数据不在正文领域，而是利用了VBA宏的案例。还有不生成HTA文件就下载Installer DLL的案例。让我们来逐一分析TA551类型Word文件在传播过程中的变形案例。

1. VBA宏代码及HTA文件的变形

查看2021年初传播的恶意Word文档，可以发现攻击者利用了VBA宏代码的用户定义样式。这与现有的利用Word正文区域的数据生成HTA文件的方式有所不同。



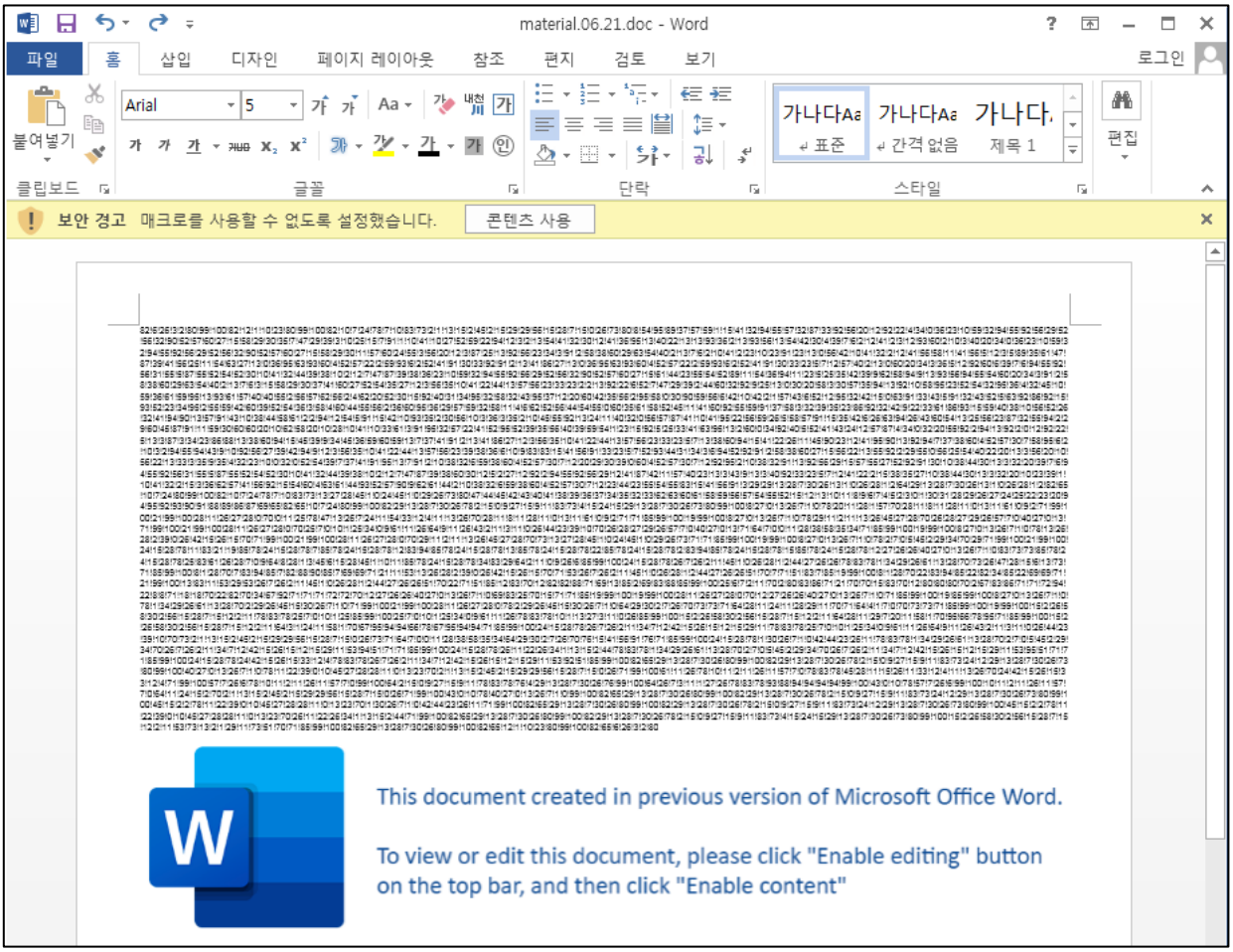
【图6】2021年2月传播的恶意VBA代码

另外，编辑设置限制也与现有方式不同，可以推测是为了使用户难以识别“诱导用户允许宏的图片”。

总的来说，在编码过程中没有使用复杂的代码混淆。攻击者基本上使用了VBA宏代码的用户定义样式和模块，对各自包含的数据，主要采用了异或运算和转换ASCII值的方式。但是，在不同时期轮番使用了能够在VBA宏代码中使用的各种编码方法，并与之前的方式混合使用，显现出了TA551类型的特点。可以推断这是攻击者为了躲避防病毒产品的检测，根据传播时期不断进行变形。

2021年3月分发的恶意Word文档是一种HTA数据存在于VBA代码中的类型， 用于传播Ursnif恶意代码。包含在HTA文件中的数据使用特定函数以排列的形式保存。此时，传播的Word文件由于编写错误的宏代码而无法正常打开。

2021年7月分发的恶意Word文档是混淆正文中的HTA数据码的类型。对正文中的数据进行编码， 宏代码也被制作为必须经过基本的运算才能解码。正文中的数据隐藏在诱导用户允许宏的图片后门，如【图7】所示。



【图7】隐藏在诱导用户允许宏的图片后面的文本

对宏代码运行过程中生成的HTA文件内数据，根据代码内容的意图进行解码时，会指定其他恶意代码下载URL及本地保存路径。对在传播过程中发现的样本进行追踪后，发现路径（path）的第一个值在很长一段时间内都统一使用了“http://[域名]/adda/~”这一格式。而且已确认下载的dll文件是在2021年7月当时运行了Trickbot恶意代码。

此外，还确认了在宏代码运行过程中不生成HTA文件，注册注册表项后直接执行VBA代码以更改宏安全设置的类型。

除了上面介绍的恶意VBA宏类型外， 可能存在更多的变形文件。可以确认会混用现有的编码及数据隐藏方式，并且不断发展成更复杂的形式。

2. 最终传播的恶意代码类型的变化

于2020年下半年发现的TA551类型Word文件主要传播了IcedID及Qakbot恶意代码。而2021年下半年开始 ，传播的恶意代码的种类又增加了。除此之外， 还从直接传播恶意代码的方式转变为通过几个阶段下载恶意代码的方式。

直至2021年上半年收集的TA551类型Word文件是通过HTA脚本代码中编码的URL直接下载恶意代码。此时下载的恶意代码主要是银行类恶意代码，如Qakbot、Bokbot、Ursnif和Trickbot等。

另外，还确认了多起在Word宏运行过程中下载两种恶意代码的案例。

【图8】下载其他恶意代码的过程

2021年9月发现的TA551类型中 ， BazarLoader DLL文件是通过HTA脚本代码中编码的URL下载的。BazarLoader DLL是一种从内存中下载后门（backdoor）并将其注入正常进程的恶意代码。然后，通过连接C2下载Trickbot等其他恶意代码。

除了TA551和Kimsuky类型外，AhnLab还发现了恶意利用外部（External）连接功能的恶意Word文档以及传播Emotet恶意代码的恶意Word文档相关内容。

结论

攻击者正不断地利用恶意Word文档发动攻击。其中， AhnLab对TA551攻击组织所使用的Word文档的运行过程及主要特征进行了重点分析。这种攻击不仅存在Word文件，还有各种类型的恶意Word文档在不断变化并传播，需要特别注意。

恶意Word文档大部分是通过邮件传播的。因此，用户在打开来源不详的邮件时需格外注意。同时还要及时更新包括V3在内的杀毒软件至最新版本，提前防止恶意代码感染。

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