

AhnLab
安全月刊

2023.12 Vol.133

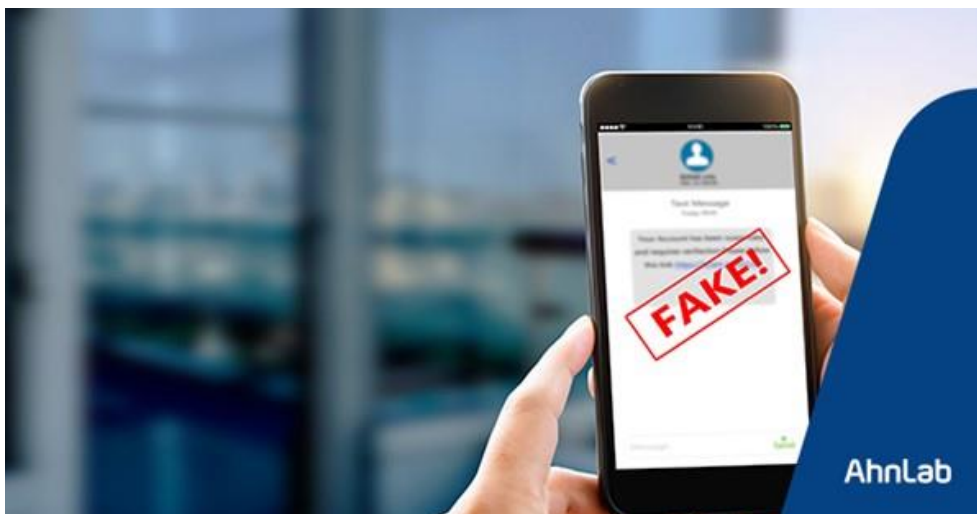
短信诈骗攻击的深入分析



短信诈骗攻击的深入分析：渗透受害者心理的恶意应用的演变

短信诈骗（smishing）已经从过去一维的欺骗方式发展为利用各种攻击技术渗透受害者心理的形式。尤其是他们制作的恶意应用设计得非常巧妙，很难轻易判断真假，因此需要更加谨慎警惕。

最近，AhnLab发布了一份深入分析韩国发生的短信诈骗和恶意应用攻击技术的报告。以下是报告的主要内容。



1.概要

随着智能手机的大众化和普及，针对智能手机的攻击也在不断增加。对于安卓设备，用户可以通过简单的步骤轻松安装从外部下载的应用程序。这进一步增加了在设备上安装恶意应用的可能性。

近来，新闻中经常报道仅通过安装恶意应用就导致受害者的资金被盗的案例。这是因为恶意应用利用了2FA（双因素认证）绕过技术导致的。2FA认证是指用户登录到其要访问的服务时，将安全码发送至事先注册的电话号码，用户输入安全码后完成身份验证，从而正常登录服务。尽管这种认证方法因其简便性而被广泛应用于网络银行账户更高和各种全球服务，但恶意应用可能会导致认证码被泄露并被滥用。

在本报告中，我们对在韩国传播的短信诈骗信息进行了分类，并总结了各类型的案例。此外，对受害者实际下载恶意应用的传播网站类型进行分类，并介绍了各网站的特点。在介绍语音网络钓鱼攻击时，我们将针对Google Play商店中存在的远程控制软件和金融资产查询软件进行详细说明，以及关于用于隐藏实际传播站点地址的缩短URL的说明，并介绍了最近3个月攻击案例中使用的缩短URL地址列表。接下来，还介绍了Infostealer（信息窃取）、Kaishi（冒充银行和杀毒软件）、Infostealer（裸聊诈骗）、SMSstealer（绕过2FA认证）等恶意应用的特点、类型、运行页面和主要功能。

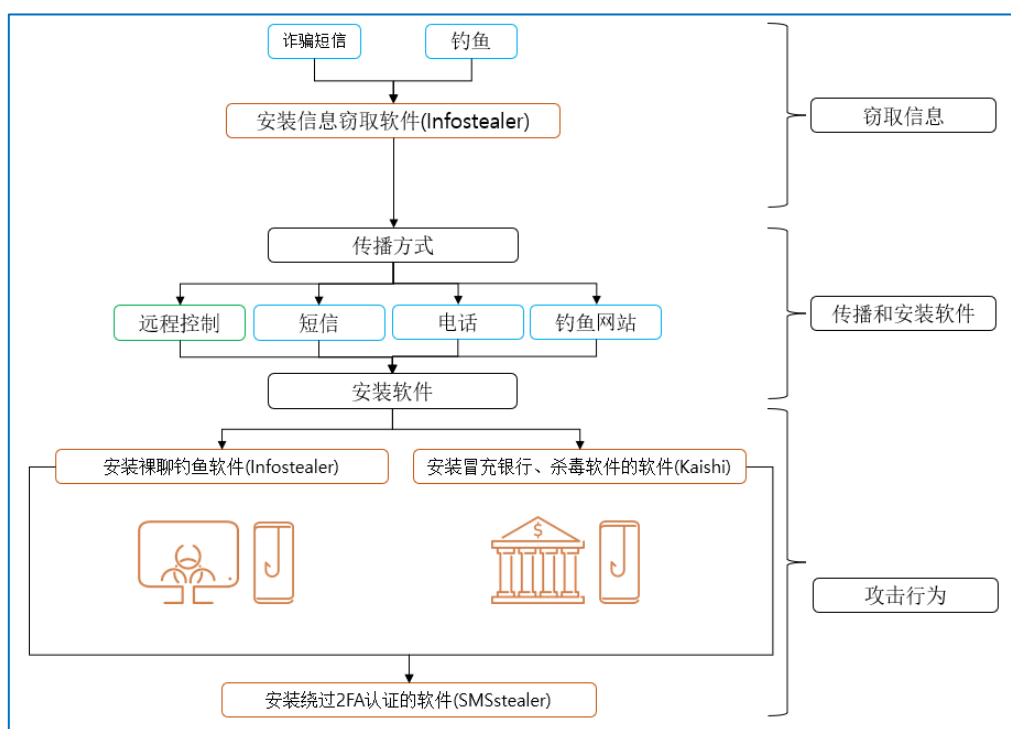
此外，通过考察各应用之间的关系，我们将介绍安装恶意应用被安装并导致用户资产泄露的场景。

2.攻击场景

发送人会通过短信或域欺骗攻击大范围发送恶意内容，来做好物色攻击目标的前期准备。受害者访问发送短信中包含的地址并安装了信息窃取软件（以下称Infostealer）后，个人信息（联系方式、短信等）敏感信息将会传送至发送人的C2服务器。

成功窃取信息后，发送人会向被感染的用户和其身边的亲朋好友发送诈骗短信，诱骗其登录钓鱼网站（恶意应用发布网站）。或者通过“涉嫌犯罪行为”、“海外结算”等可能引发受害者不安的言语迷惑受害者，诱导其安装远程控制软件后，再以“终端检查”等理由安装并运行伪装成银行或杀毒软件的应用程序（以下称Kaishi）。又或者伪装为成人聊天或约会软件，利用受害者想要看到更多信息的心理，诱导其安装裸聊软件（以下称Infostealer）。

发送人的目的是为了诈骗钱财，为了绕过2FA认证流程，会诱导受害者安装拦截信息的恶意应用（SMSstealer）。由此可知，目前诈骗方式已经发展成从安装了Infostealer和Kaishi的受害者终端设备窃取认证码来盗取资金的形式。攻击者利用的攻击方法和恶意应用信息以及攻击场景整理如[图1]所示。



[图1]攻击场景

[图1]中的蓝色部分是攻击方式，每种方式的介绍如下。

- **短信诈骗**：通过短信诱导访问钓鱼网站来传播恶意代码的方式。
- **域欺骗**：在中间窃取正常网站的域名地址（DNS），使用户以为自己访问的是正常网站，从而窃取个人信息的方式。
- **钓鱼**：面向非特定大规模人群，通过访问虚假网址窃取个人信息的攻击方式。

[图1]中的绿色部分是攻击正常应用程序使用的方法，具体如下。

- **远程控制**：攻击者控制安装了远程控制软件的受害者设备。通过远程控制执行安装软件、监控终端等行为。

[图1]中的红色部分是攻击中使用的恶意应用，各软件的特点如下。

- **窃取信息的Infostealer恶意应用**：窃取个人信息的恶意应用，通常伪装成快递、商城等。
- **裸聊诈骗的Infostealer恶意应用**：窃取终端设备信息和个人信息后，进行实时录音和录像等操作的恶意应用，主要伪装成成人应用程序。
- **冒充银行和杀毒软件的Kaishi恶意应用**：窃取终端设备信息和个人信息等后，将默认电话软件转换成恶意应用来监控电话状态。设有监视电话号码的列表，具有“强接强打”（强制接听、强制拨打）的功能，控制用户拨打诈骗人员不希望的号码或不接听电话、接通电话等电话的相关操作。主要伪装成银行软件。
- **绕过2FA认证的SMSstealer恶意应用**：将默认信息软件转换成恶意应用后，监控终端设备的收信和发信状态。它可以窃取被感染的终端设备收发的所有消息，因此不存在消息记录，所有消息的内容都被泄露。主要伪装成快递、请帖等应用程序。

3.攻击方式

下面将介绍攻击者传播恶意应用后，从安装到运行使用的攻击方式以及攻击时使用的正常软件和服务。

3.1.诈骗短信

诈骗短信的形式不断进化，它抓住受害者的恐惧心理，散布社会问题、个人生活相关的内容，诱导其安装恶意应用。诈骗短信主要以包含内容和恶意URL链接的地址的形式进行传播，近来，为了绕过安全程序的检测，其形式进一步发展，删除了URL地址，代之以攻击者的电话号码，要求受害者打电话。

短信内容大部分包括“国外发送”、“Web发送”等，为了防止被杀毒软件监测，会采用在正常词语中插入不必要的字符、删除空格、使用奇怪字符等方法。为了避免受害者生疑，下载恶意应用的地址会使用URL快捷方式提供服务。

3.1.1.快递诈骗

大多数快递类型的诈骗短信主要采用冒充快递公司的方式。虚假短信以“国外发送”、“国际短信”、“快递单号”等信息开头，通过“道路名称不一致，需要变更地址”、“配送延迟，需要确认配送时间”、“查看未收件快递”等词语造成受害者的焦虑情绪。访问短信中给出的地址后，会显示冒充快递公司的钓鱼网站。因此，受害者为了确认信息，会在毫无戒备的情况下输入电话号码、姓名、出生日期等信息后下载并安装包含恶意行为的软件。

近来，快递公司不再使用短信发送快递运输通知，而是通过自主开发的应用程序或门户网站提供通知服务，请务必留意。收到冒充快递公司的消息后，应当通过快递公司提供的运单查询服务直接确认，防患于未然。

3.1.2.冒充公共机关

冒充公共机关的诈骗短信主要以最近的社会热点或警察和公团等的名义发送，通过“交通违章”、“犯罪报告”、“罚款”、“通知书”等词语造成受害者的焦虑情绪。访问短信中给出的地址后，会显示冒充机关的钓鱼网站。因此，受害者为了确认信息，会在毫无戒备的情况下输入电话号码、姓名、出生日期等信息后下载并安装包含恶意行为的软件。

请务必牢记，除官方应用商店外，公共机关不会让用户从其他地方安装软件。收到冒充公共机关的诈骗短信时，应当与发信机关的接待中心进行核实，防止受骗。

3.1.3.冒充亲友

冒充亲友的诈骗短信包含“请帖”、“婚礼”、“讣告”、“认证”等词语，看起来像是受害者真正的亲友发送的。如果短信中包含地址，会诱导受害者访问；如果不包含地址，则会通过短信或电话以身份认证的名义要求提供身份证照片等个人信息或者添加特定的SNS账户。收到冒充亲友的诈骗短信时，应与亲友取得联系，确认消息是否确为其所发，以防上当受骗。

3.1.4.结算诈骗

结算诈骗短信不同于其他类型的诈骗，它没有钓鱼网站地址。如果包含地址，可能会引起怀疑，所以为了诱导受害者打电话，主要以发生了大额支出的内容造成受害者的焦虑情绪，并诱导其拨打电话。拨打短信里的电话号码时，会连接至假冒的客服中心而不是真正的客服中心，对方会以受理损失投诉的名义要求提供电话号码、姓名、出生日期等信息。这并不单纯是为了收集个人信息，而是诈骗的一环，来确认攻击者是否确实将相关短信发送给受害者。

攻击者会基于已经掌握的个人信息发送诈骗信息。受害者拨打电话后，攻击者确认其是否是自己传播信息的对象，如果一致，再诱导其安装远程控制软件或以检查手机的借口要求安装其他软件。由于攻击者使用的电话号码会在平均几个小时后停用，但在经过一段时间又可以作为正常号码使用，所以，不要只通过号码查询结果来判断是否属于诈骗，更重要的是应当删除可疑短信。收到结算诈骗短信时，应向发卡客服中心确认是否存在结算行为，如果不存在结算项目，则务必删除短信，以防受骗。

3.1.5.冒充金融机构

冒充金融机构的诈骗短信一般包括贷款、社会热点等内容。此前，诈称新冠肺炎补助金的短信曾流行一时，一般情况下有关贷款的内容较多。过去，冒充金融机构的诈骗短信会诱导受害者访问可以下载恶意应用的钓鱼网站。

最近，为了诱导受害者直接向攻击者拨打电话，短信中会包含电话号码，同时包含真实的银行客服中心号码和“直拨号码”、“咨询”、“免费拒收”等内容以及虚假号码。拨打虚假号码（攻击者）时，通过语音提示告知冒充银行的钓鱼网站地址，诱导受害者直接访问并安装应用程序。收到冒充金融机构的诈骗短信时，应联系金融机构客服中心告知具体情况并确认是否发生损失。

3.1.6.其他类型

其他类型的诈骗短信传播元素包括裸聊、社会热点等。在裸聊诈骗的情况中，攻击者冒充会员与受害者联系，声称要查看更多信息就必须安装应用程序，然后直接发送恶意应用或跳转至可以安装的网站。此外，也会恶意利用社会热点或受害者恐惧的因素散布诈骗短信。收到这类不必要的信息时，应予以删除，防止受骗。

3.2.恶意应用传播网站

恶意应用传播网站的攻击方式较为多样，会让用户直接安装应用程序，或者只要访问网站即可下载恶意APK等。这些传播网站的共同特点是冒充特定机构或企业，或者伪装成成人网站等运营。另外，为了看起来像正常网站，它们会设计成输入受害者电话号码、运单号码等信息后即可查看所需信息的形式。

大部分的传播网站在除手机外的其他环境（Windows PC等）下访问时，会跳转至正常网站。请务必注意，虽然攻击者直接开设网站诱导访问的形式依然存在，但利用正常网站的功能诱导受害者访问的案例屡见不鲜。

下面对各种恶意应用传播网站的形式进行了整理。

3.2.1.输入电话号码

诱导输入电话号码的钓鱼网站是最普遍的恶意应用传播网站类型之一。通过快递、健康体检、交通管制等各种形式的诈骗短信跳转至输入电话号码、运单号码的网站。以往，在传播网站输入信息（电话号码、运单号码等）时，不会单独进行检查。但是，近来诈骗方式进化，如果不是攻击者传播对象的电话号码、运单号码、姓名、出生日期等，则无法下载恶意应用。

3.2.2.点击按钮

点击按钮的传播网站为了让用户直接安装应用程序，主要使用“打开”、“下载”、“官方商店”等按钮。有的案例是在点击官方商店按钮时会跳转至似乎是真实商店运营的虚假网页。通过点击按钮传播恶意应用的网站，可以在不经认证的情况下将恶意应用下载至终端设备。

3.2.3.直接下载

针对诱导下载类型的传播网站，当访问散布者发送的地址时，会直接从终端设备下载恶意应用。受害者无法决定是否下载，攻击者可以通过远程控制在终端设备中安装下载的APK文件。

3.2.4.重定向

重定向的方式是通过部分SNS允许的重定向功能访问正常网站地址时连接至恶意应用传播网站。攻击者向受害者发送包含正常链接地址的信息，如果受害者访问链接，即被重新定向至恶意应用传播网站。由于使用该功能时是隐藏在正常网站地址中，因此，受害者无法分辨链接是否属于恶意链接，很可能遭受损失。

```
<!-- Inside head -->
<meta name="description" content="Redirection Test">
<script type='text/javascript'>
  let new_slug = window.location.pathname;
  let new_root = "████████████████████";
  let new_url = new_root + new_slug;
  console.log(`<link rel="canonical" href="\`" + ${new_url} + "\`">`);
</script>

<script type='text/javascript'>
  window.location = new_url;
</script>
```

[图2]重定向网站的类型

3.3.攻击时使用的正常软件和服务

过去，攻击者只是通过诈骗短信中的地址诱导受害者访问恶意应用传播网站。但是，由于杀毒软件检测、智能手机用户的安全意识提高等，很难成功攻击。

如此一来，攻击者为了达到成功攻击的目的，不再采用直接发送恶意应用传播网站地址的方式，而是开始利用URL快捷方式服务或者首先让用户从官方商店安装软件，避免用户起疑。另外，攻击者还会采用直接远程连接受害者设备后再访问恶意应用传播网站下载恶意应用的形式。同时，为了轻松掌握资产情况，他们会通过提供服务的资产查询软件快速了解受害者的资产情况，确认可以盗取的资金数量。

接下来，将对攻击者主要使用的远程控制软件和金融资产查询软件的种类及特征进行介绍。

3.3.1.远程控制软件

攻击者会利用两点通过远程控制软件进行攻击。第一点，通过官方商店下载软件。攻击者诱导受害者在官方商店下载远程控制软件，既然是官方商店中下载的软件，受害者下载远程控制软件时也就不会有所怀疑。

第二点，为了掌握受害者的情况，以亲自查看终端设备的名义要求安装远程控制软件。受害者在遇到不知所措的情况时，有人虚情假意地表示可以为其检查终端设备，便会感到安心，从而按照攻击者的要求安装远程控制软件。攻击者直接访问受害者的设备，可以轻松安装恶意应用，也可以查看金融信息等个人信息、确认是否安装了杀毒程序。

下面是一些经常用于攻击的远程控制软件。

3.3.1.1. TeamViewer QuickSupport

TeamViewer QuickSupport是一款Google Play商店中下载次数达5000万次的热门远程控制软件。安装QuickSupport后，只需完成同意使用的流程，既可分配用于控制终端设备的专属ID信息，并可使用该ID信息通过网页或安装了Teamviewer的其他终端设备进行控制。

攻击者在与受害者接通电话后，便会诱导其通过Google Play商店安装QuickSupport，并在运行此软件后要求提供专属ID信息。通过ID设置远程控制环境后，受害者的设备上会显示“允许远程控制”、“读取通知窗口页面中的所有信息”窗口，攻击者再诱导受害者点击允许按钮。正常进行远程连接后，软件存在显示点击了设备中哪个页面的功能，可以实时查看设备的页面状态。

3.3.1.2. TeamViewer Host

TeamViewer Host在Google Play商店中的下载次数超过500万次，与其他Teamviewer软件相比，下载数较少，却经常被攻击者使用。与前文介绍的QuickSupport不同，运行此软件时需要用TeamViewer账户登录，以便添加设备。攻击者用自己使用的账户登录软件后，在攻击者的账户中将受害者的终端设备注册为可以信任的设备。登录完成后，通过攻击者使用的终端设备上安装的TeamViewer程序开始远程控制。与QuickSupport不同，开始远程控制时，它只显示“允许远程支持”窗口，点击允许按钮即可进行远程控制。

3.3.1.3. AnyDesk

AnyDesk在Google Play商店中的下载次数超过5000万次，其和TeamViewer QuickSupport一样，是非常热门的远程控制软件。运行此软件时，有的终端设备要求安装其他插件，插件需要授予访问权限，以便更好地进行远程控制。正常授权后，会显示使用

同意书和可以连接设备的专属地址。网站或移动设备发来远程控制连接请求时，弹出安全警告窗口，点击允许截屏后，即可进行远程控制。

3.3.2.金融资产查询软件

攻击者的最终目的是盗取受害者的资金。因此，攻击者需要确认选择的对象是否拥有一定数额的现金。以往，必须向受害者——询问使用哪家银行、在各银行的账户信息和名下金额等。近来，可以更加简单方便地查询个人资产的资产查询应用程序出现，攻击者便使用这些应用程序确认受害者的资产信息。

3.3.3.URL快捷方式

URL快捷方式被称为“域名缩短服务”，可以通过快捷方式提供以往的域名地址。以往的域名地址长且复杂，所以主要用于短信或部分SNS限制字数而无法发送地址信息时。诈骗短信散布者通过URL快捷方式隐藏恶意应用传播网站地址，让受害者无法通过URL快捷方式判断链接的真伪。最近3个月内收集的诈骗短信使用的URL快捷方式列表见表7。

URL快捷方式列表
me2.do
abit.ly
ko.gl
urlzs.com
snip.ly
dokdo.in
xgo.kr
t.ly
bit.ly
han.gl
zrr.kr
vvd.bz
surl.li
bitly.com
s.id

[表1]近期使用的URL快捷方式列表

综上所述，攻击者基于升级版攻击方式，巧妙地利用受害者的心理，进行各类攻击。为了预防短信诈骗和恶意应用造成的损失，必须预先安装手机杀毒软件，并持续更新。另外，不要访问可疑的网站，并养成删除来源不明的短信的习惯。



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

© 2023 AhnLab , Inc. All rights reserved.