AhnLab

# 安全月刊

2021.12 Vol.109

2021 年安全威胁总结

# 2021 年的安全威胁，对变化做出“敏感反应”

去年底，AhnLab发布了2021年安全威胁预测Top 5：▲针对性勒索软件的扩展和高级化▲新冠疫情所改变的工作环境和安全威胁▲恶意代码编程语言的多样化▲恶意代码运行方式的模块化▲恶意应用程序针对国家的扩大。如今，一年已过，让我们总结一下2021年，看看哪些安全威胁已经成为了现实。


勒索软件、国家资助的黑客组织和移动恶意应用程序近年来成为了主流攻击趋势，在2021年仍呈上升趋势。有所改变的是，此类主流对新的问题和新的基础设施做出了更加“快速且灵敏”的反应。当发生社会的问题时，无论攻击路径和目标平台如何，都会直接利用这些问题进行社会工程学攻击。

2021年的主要安全威胁可以归纳为五大类：▲国家资助的黑客组织活动及其造成的破坏在继续▲针对型勒索软件的攻击和其破坏规模的增加▲大量传播已升级的文档型恶意代码▲利用社会问题进行社会工程学攻击活动▲金融移动恶意应用程序试图不断改变

## 1.国家资助的黑客组织活动及其造成的破坏在继续

一些黑客组织为了本国利益，试图对国内外的公司、政府机构和教育机构进行攻击。2020年，国家资助的黑客组织专注于针对开发新冠病毒疫苗的制药公司尝试进行攻击。2021年，将目标范围扩大到包括医疗、国防、研究机构、政治和安全等多个领域。特别是在研究机构、医疗和国防领域，因黑客攻击而发生的数据泄露事故是众所周知的。这些国家资助的黑客组织利用VPN（Virtual Private Network）和集成管理等公司专用解决方案中的漏洞进行攻击。

大多数这些黑客攻击始于邮件，主要是冒充门户网站的网络钓鱼、恶意脚本和包含恶意宏的办公文档附件。在一些事例中，还报告了恶意利用Adobe PDF漏洞（CVE-2020-9715）和MS Office漏洞（CVE-2021-40444）的事例。获得国家资助的黑客组织使用的MS Office漏洞（CVE-2021-40444）目前被普遍使用，Magniber勒索软件是具有代表性的恶意代码。

## 2.针对型勒索软件的攻击和其破坏规模的增加

从恶意代码的角度来看，依然是勒索软件抢占了所有问题。2021年，无论是国内还是国外，勒索软件攻击的数量和造成的损失额也显着增加。特别是，针对企业的针对性攻击大幅增加，而不是针对个人PC的攻击。利用美国石油管道公司Colonial Pipeline和软件公司Kaseya供应链的勒索软件攻击是今年的重大安全事件。根据美国财政部宣布，2021年上半年由勒索软件攻击造成的损失额（约7千亿韩元）超过了2020年的总损失额（约5千亿韩元）。

在韩国，包括大型企业和大学医院在内的许多企业均受到了勒索软件的攻击。如果查看2021年AhnLab收到的勒索软件攻击事例，可以发现其类型和传播方式非常多样化，从利用漏洞的Magniber勒索软件到利用附加到电子邮件的诱饵文件的勒索软件。这种以企业为目标的针对型勒索软件攻击预计将在2022年继续发生。

另外，在执法部门的努力下，勒索软件制作者已被陆续逮捕，现有勒索软件组织的活动也被宣布停止。1月Net Walker勒索软件、2月Egregor勒索软件、6月Clop勒索软件、10月LockerGoga、MegaCortex、Dharma勒索软件涉案嫌疑人已均被逮捕。但是，一些宣布停止活动的组织可能会以不同的名称继续活动，这可以解释为一种躲避跟踪的手段。

## 3.大量传播已升级的文档型恶意代码

在2021年，通过现有方法升级的文档型恶意代码不断传播。代表性的文档类型有Word、Excel、PowerPoint和PDF，并且不分针对型和非针对型，每个案例的传播目的都是多种多样的。

这些文档型恶意代码通常以网络钓鱼的形式通过电子邮件分发。有时在文档内容中包含针对特定人物的特定主题，因此用户毫无怀疑地运行它们。还有些文档诱导运行宏，目的是将恶意代码分发给非特定人群。总之，泄露用户信息的文档类型很多。例如：▲窃取银行信息的恶意代码Trickbot和Dridex▲从Web浏览器、FPT客户端、即时通讯工具和加密货币钱包中窃取数据的KPOT▲泄露存储在Web浏览器、邮件和FTP客户端等的用户信息的AgentTesla。还有一种情况，感染后门或RAT类恶意代码为目的是为了从最终连接的C&C服务器的攻击者接收额外的命令，而它们并非是泄露信息类型。

这些类型的文档型恶意代码为了绕过文件诊断和行为诊断，通过增加恶意宏代码混淆的复杂性或增加运行进程中的阶段以不断变化形态。

## 4.利用社会问题进行社会工程学攻击活动

2021年，以各种社会问题为关键词的网络攻击不断被发现。在韩国，用于攻击的主要问题分别是新冠状病毒疫情和相关问题、与朝鲜相关的政治和社会问题以及与股票相关的经济问题。

攻击是通过恶意利用大多数公众所感兴趣的诸如新冠状病毒感染者的移动路线、灾难基本补贴和支持个体户的综合指南等关键词来进行的。此外，与朝鲜有关的关键词，如朝美首脑会谈、中国军事战略分析、安全研讨会、朝韩交流等，也是有效攻击的关键词。特别是，由于加密货币和股票市场的兴起、非面对面交易以及各种网络资产的出现，针对经济问题的网络攻击也随之而来。并且，通过Netflix在全球范围内流行的电影“鱿鱼游戏”以及对前总统的吊唁等焦点问题也被攻击者利用。

需要注意的是，这样的社会工程学攻击不是技术攻击方法，而是利用人的心理进行的攻击，因此取决于用户的粗心和失误。因此，最好禁止访问在短信或电子邮件中来源不明的URL地址，并使用经过广泛验证的网站或服务平台进行重大新闻文章和信息搜索。

## 5.金融移动恶意应用程序试图不断改变

金融类移动恶意应用程序也改变了攻击对象和恶意应用程序的创建方式。Trojan/Android.Kaishi是针对韩国国内用户的代表性金融恶意应用程序，自2014年开始出现，但最近改变了该应用程序的创建方式，对攻击对象进行了精确管理并增加了损害。它被用于语音钓鱼的应用程序，保留了操作电话的核心功能，但发现其应用了代码混淆、打包、加密等应用程序安全技术，呈现出与现有的应用程序完全不同的结构。这可以解释为避免检测并提高攻击成功率的手段。

一般来说，金融类恶意应用程序的攻击对象是银行应用程序。但可以看出，最近在海外报道的金融恶意应用程序的大部分对象中还包括如购物应用程序，以及与加密货币相关的在线金融服务应用程序。这些恶意应用程序

旨在劫持加密货币服务的用户帐户或窃取身份验证密钥。由于实际信息被盗而造成经济损失的事例正在逐渐增加，因此有必要关注随着金融科技服务的增加和扩展而蠢蠢欲动的新型移动恶意应用程序的出现。

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