网络安全报告

2020年总结

2021年预测

AhnLab

网络安全报告

2020
威胁总结

2020年值得关注的网络安全威胁Top 5

AhnLab

01
勒索软件已经很熟悉，受害仍然严重

从几年前开始，勒索软件一直出现在该年度的威胁总结和下年度的预测中。虽然勒索软件已广泛传播，已经达到人们对它已经很熟悉，但受害情况仍然十分严重。在2020年，使用针对性勒索软件的攻击组织的壮大尤其引人注目，他们在加密文件之前先窃取内部信息并声称将其泄露给外部，以此来施加“双重压力”。

去年，在全球范围内受到关注的两起勒索软件受害事例如下。

A. Maze（迷宫）勒索软件，发动全球性的攻击

首先，Maze（迷宫）勒索软件对全世界的企业发起了针对性攻击。攻击组织在窃取企业内部的数据后索要钱财并进行威胁，如果受害企业不回应，则在自己的网站上公开窃取的数据。11月初，Maze（迷宫）勒索软件组织宣布隐退时，以删除数据作为条件，要求企业在指定期限内与他们联系。

B. DoppelPaymer勒索软件，夺走患者生命

去年9月，在德国杜塞尔多夫大学医院发生的勒索软件攻击使医疗系统瘫痪，导致急诊患者死亡。由于30台医院服务器被勒索软件感染，因此大部分医疗服务被迫中断，并且延误了治疗，导致急诊患者死亡。此后，德国调查机构透露，攻击医院的是一种名为“Doppel-Paymer”的勒索软件。尽管患者的死亡并非攻击组织的故意行为，但该事件表明，如果主要基础设施被勒索软件等恶意代码感染，稍有不慎就会危及生命。

02
受到国家资助的黑客组织的全方位攻击

今年，也有许多黑客组织为了本国的利益，试图攻击国内外企业、政府机关、大学和个人。一些企业的员工帐户信息和内部数据被泄露，对于个人而言，持有的虚拟货币被盗。

在国家资助的黑客组织的趋势中，新冠病毒是必须提及的关键词。随着全球的新冠病毒感染者暴增，跨国制药公司争相开发新型冠状病毒疫苗（以下简称为新冠疫苗），许多黑客组织试图针对政府机关和制药公司进行攻击。

欧洲药品管理局（European Medicines Agency：EMA）一直是黑客攻击的目标，他们试图窃取与其保管的新冠疫苗有关的文件。另外，不断地报告疑似受到特定国家规划性资助的攻击组织，非法获得新冠疫苗技术、研究结果和冷链（低温运输系统）的事例。

常年以来一直是全球黑客组织目标的Hangul文档（HWP）漏洞与去年相比有所减少。其原因推测为，攻击者使用的Hangul文档中的Ghost脚本漏洞已通过Hangul程序的安全更新消除，并且随着时间的流逝，用户的Hangul安全更新的安装被普及，因此判断攻击很难再有效。但是，作为一种替代攻击方案，扩大使用了宏病毒（Macro）、PowerShell、Windows脚本文件（WSF）和VBScript等脚本恶意代码。

03
更精心设计的网络钓鱼攻击

今年发现的网络钓鱼（Phishing）型恶意代码发展地更加精致，可以更容易欺骗用户。伪装成正常门户网站的恶意网页会将登录界面伪造成正常网站，从而欺骗用户并试图窃取帐户信息。在过去，界面的构成多少有些粗糙，但如今界面已经变得如此精致，以至于即使专家也很难区分真假。这种网络钓鱼型恶意网页会在用户输入帐户信息后，将信息发送至服务器，然后重定向（redirect）到正常网站，从而防止了用户的怀疑。

电子邮件也是如此。主要与业务相关的内容（例如“系统检查指南”、“限制帐户访问”、“订购单”），使用户毫无疑虑地点击恶意链接或运行邮件中的恶意附件。过去，垃圾邮件以英文编写并广泛发送给非特定多数的对象，但是，最近发现了许多用韩文编写并为用户量身定制的内容。可以看出，恶意代码的制作者正在制作并传播更精心设计的网络钓鱼型恶意代码，以提高攻击成功率。

04
僵尸网络(Botnet)恶意软件的大量传播

以Emotet恶意软件为代表的僵尸网络恶意软件已在全球大量传播。僵尸网络恶意软件是一种在感染众多用户后，根据攻击者的命令进行操作的恶意软件，执行诸如泄露用户信息和下载其他恶意文件之类的功能。

Emotet恶意软件最初是一种金融信息泄露型的恶意软件，但后来逐渐演变为下载并运行泄露其他金融信息的恶意软件，例如TrickBot和QBot。2020年发现的大部分僵尸网络恶意软件都是通过恶意电子邮件传播的。当运行插入到电子邮件附件中的宏时，恶意文件被下载。

僵尸网络恶意软件通常是通过生成器生成，因此，每隔几个小时会非常快速地进行附件文档文件和可执行文件外型的更改。另外，由于该功能必须收到攻击者的命令后启动，因此很难掌握恶意代码的最终目的，而且每个用户的受害情况根据运行时间而变化的特征。

05
通过供应链传播的恶意应用的增加

2020年通过Google Play传播的恶意应用程序的类型和数量大幅增加。经证实，以这种方式分发的恶意应用程序主要执行诸如盗取金融信息、加入订阅服务和分发广告之类的功能。

在使用WAP（无线应用通讯协议）收费服务的国家/地区，在用户不知情的情况下加入收费服务的“Trojan/Android.Joker”于2020年首次被发现后，通过伪装成文件扫描仪或相片编辑器等软件并通过Google Play不断分发。恶意应用Cerberus的源代码由恶意代码制作者公开，同样通过Google Play不断分发。

植入广告型的恶意应用程序首先会为游戏或其他用户提供有用的功能。并且在召集了许多用户之后，根据从攻击者服务器（C2）收到的命令立即植入攻击性广告。因此，通过Google Play传播的恶意应用程序具有导致许多受害者的特征，因为它们在启动恶意功能之前需要等待一段时间（潜伏期）。

网络安全报告

2021
威胁预测

2021年网络安全威胁趋势Top 5

AhnLab

01
针对性勒索软件的扩大和发展

到目前为止一直活跃的Maze（迷宫）勒索软件在11月初宣布隐退。但是，这仅是在众多勒索软件威胁中的一个消失而已，其他勒索软件势必会填补这个空缺，并且损害也将继续。特别是，针对性勒索软件组织极有可能通过相互合作来扩展其功能并提高攻击强度。对于网络犯罪组织而言，勒索软件是一种重要的赚钱工具。

如今，企业为提高资源管理的便利性和效率，通常会使用各种软件。但是，如果软件中存在漏洞，则被攻击者利用它来掌握企业内部情况并创造可以执行恶意行为的环境。攻击者不断升级其方式，以逐步有效地进行渗透、掌握和窃取等攻击。

回顾过去通过媒体已知的韩国国内黑客事件，也有黑客利用企业版软件漏洞的事例。勒索软件攻击也是一种极有可能的情况，在2021年，可以预测更高级、更活跃的勒索软件的传播。

此外，无法保证在韩国不会发生因上述勒索软件攻击导致的医疗系统瘫痪而导致急诊患者死亡的事件。为此，必须增强安全系统、遵守安全守则以及提高安全意识。

02
新冠状病毒改变的工作环境以及随之而来的安全威胁

自新冠病毒爆发以来转眼已经过去了一年。2020年，由于新冠病毒，人们的生活方式发生了巨大变化。例如，网上购物和送货服务的使用急剧增加，并且不受场所限制和远程进行的“无接触（非面对面）”商务活动也大大增加。

在非面对面的工作环境中，与受企业安全策略保护的情况不同，每个成员是主体，这就需要更加注意安全。但是，由于费用和人力等方面的原因，实际上不容易做到。从安全方面来看，新冠病毒对企业而言是新的挑战，同时对攻击者而言是机会。在2021年，预计针对非面对面工作环境的网络钓鱼和针对性攻击将继续发生。

对此，企业需要认识到在无接触环境中的安全系统的必要性而不是建议，并在该环境中明确设置安全的优先级。另外，在使用VPN（Virtual Private Network）时，需要设置正确的策略并加强用户验证，还可以考虑引进无需专业安全人员即可有效创建安全的工作环境的SaaS（Software as a Service/软件即服务）型的安全解决方案。

03
制作恶意代码的编程语言的多样化

预计在2021年，EXE和DLL等可执行文件的恶意代码的制作方式将变得更加多样化。从过去到现在，许多可移植的可执行文件（Portable Executable）文件都以C、C++、Visual Basic、Delphi、C#等编程语言制作，但最近却出现了很多使用Python或GoLang等编程语言制作的恶意代码。

可以看出，攻击者似乎充分利用了易于编译和二进制生成以及相对容易添加其他库或模块的优点。另外，由于文件的形式和结构与现有防病毒产品的特征码模式完全不同，因此，预测攻击者会针对这点制作恶意代码。

04
恶意代码运行方式的模块化

恶意代码的运行方式已经正在被模块化。不是一个文件执行攻击者C2服务器通信、下载、信息泄露和文件创建等操作，而是将这些功能分成多个文件执行。这不仅是为了最大限度地躲避防病毒检测，也是为了能更长时间地维持其恶意功能。例如，如果有一个单独的文件从攻击者服务器下载已编码的文件并对其进行解码，则仅通过查看单一文件的信息是很难掌握其正确功能和恶意行为流程。

在2021年，预计这种模块化的恶意代码会增加。特别是，它们将诱导用户访问恶意服务器并下载文件，并通过不断更换植入的文件来造成损害。

05
恶意应用所针对的国家/地区范围的扩大将加速

针对移动终端的恶意应用程序，由于语言和文化差异以及支付系统的多样性等原因，往往仅在单一国家实现有效的攻击。攻击韩国智能手机用户的网络钓鱼应用程序（Dropper/Android.PhishingApp）通过快递、请帖、新冠病毒等社会热门相关的钓鱼信息传播。该恶意应用程序泄露保存在用户智能手机中的信息，并将其用于电话诈骗来诈取钱财。

2020年，在多个国家确认了疑似由同一制作者执行的恶意应用程序的传播事例。攻击者使用了伪装成各国代表快递公司的方法。另外，还证实了伪装成知名的内容提供商（例如Netflix和Disney）或知名度高的游戏来进行传播的恶意代码和使用户订阅浏览器提示广告的恶意代码。

这种恶意代码可能会传播到多个国家的用户，因为广告提供商会为终端所在的各国语言提供广告。过去，由于获利有限而仅在局部地区运行的恶意应用程序已开始针对多个国家的智能手机用户，并且预计这种趋势将加速。

网络安全报告

2020年总结
2021年预测

发行 AhnLab, Inc.
起稿 AhnLab 安全应急响应中心(ASEC) ASEC响应组
编辑 AhnLab 内容企划部门

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

AhnLab.com

AhnLab