AhnLab

安全月刊

2020.07 Vol.92

2020 年上半年安全威胁

© AhnLab, Inc. All rights reserved.

2020年上半年安全威胁

上半年的安全威胁在很大程度上受到了 2019 新型冠状病毒的影响

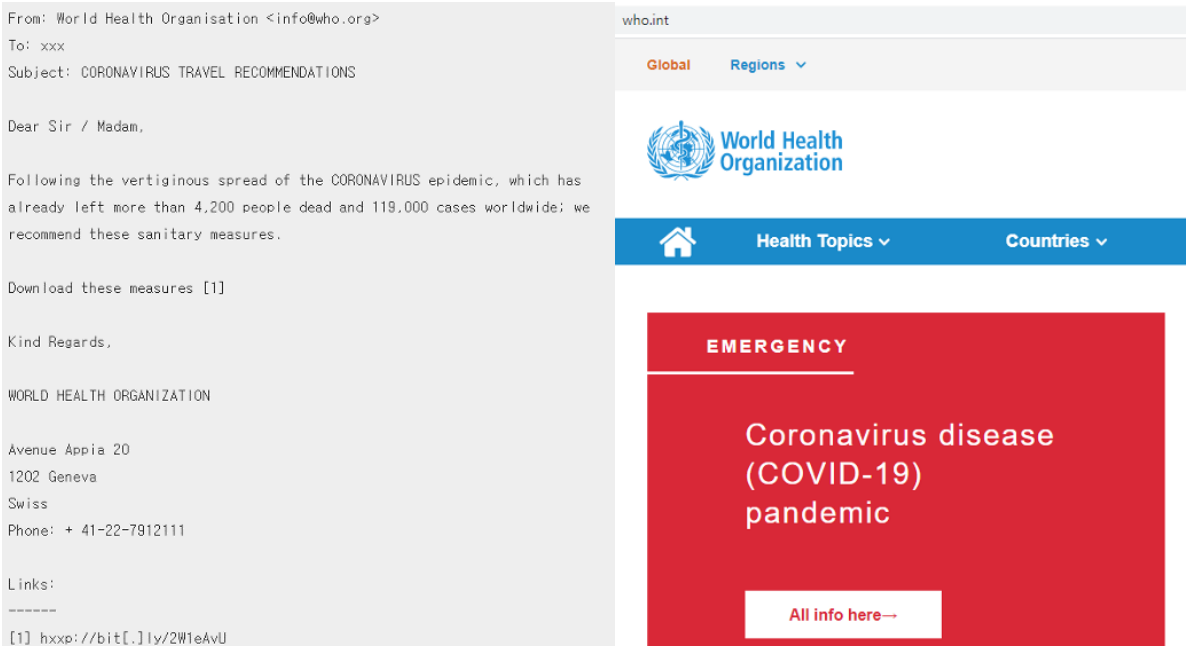
2020年伊始，曾有预测在东京奥运会赛季前后，可能会出现国家网络安全威胁。但出乎所有人的预料，生物病毒“2019新型冠状病毒（COVID-19，以下简称为新冠病毒）”的出现，导致全世界发生了剧变。如果说该传染病彻底改变了我们生活的方方面面，这话一点也不为过。曾经为了隔离沙尘暴和雾霾而戴的口罩，如今成为了每时每刻都要使用的必需品。在户外活动时，应尽量避免与对方面对面用餐，尽可能减少对话，即保持社交距离，还要在生活中保持距离，这样才能在当今时代健康地生活下去。通过远程授课和远程办公，使非面对面、非接触成为司空见惯的方式，人们生活也不可避免地发生了变化。虽然实践保持社交距离及生活距离，给社会各个部分带来了不便的因素；但为了所有人的健康，也有必要忍耐这段时间。既然我们的日常生活变得有些不方便，那么在网络空间里，我们的生活又如何呢?

本文将介绍因新冠病毒而面临剧变的2020年上半年的IT安全方面有哪些威胁成为了焦点。

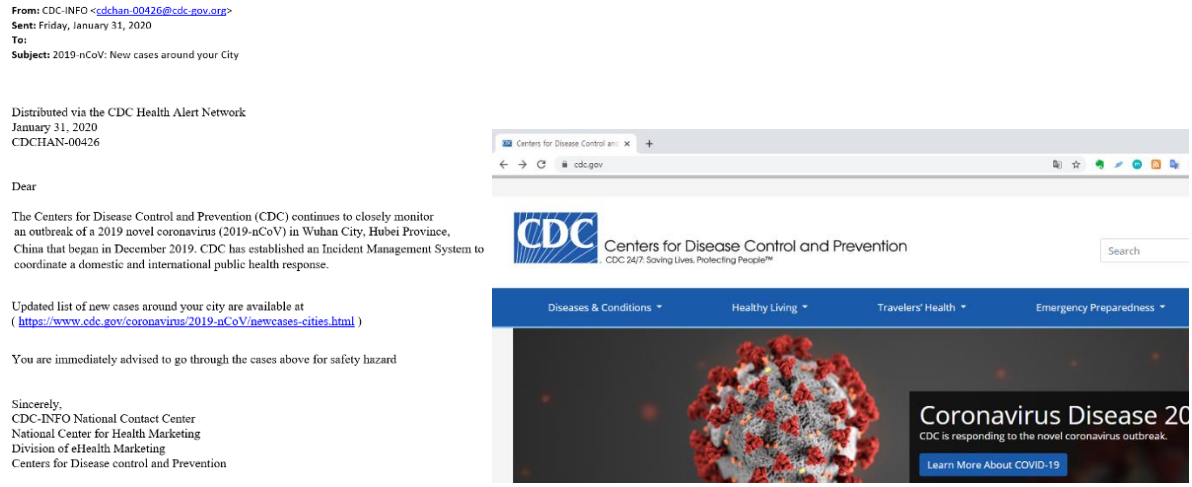
1. 伪装成新冠病毒信息的网络攻击

世界卫生组织（The World Health Organization，以下简称为世卫组织）于 2020 年 3 月 12 日正式宣布，新冠病毒已进入传染病第 6 阶段，即全球大流行（Pandemic）阶段。并敦促个人和国家要积极对抗这一威胁，以战胜不仅限于公共卫生领域，也包括对社会、经济在内的所有领域造成负面影响的混乱时期。趁着这一混乱时期，网络攻击势力的矛头也正巧妙地开始对准着我们的周围。其中最具代表性的网络威胁是伪装成新冠病毒信息的网络攻击。伪装成含有新冠病毒相关信息的电子邮件恶意代码，将电子邮件发件人的地址写成类似于世卫组织或美国疾病预防控制中心（CDC）的地址，以蒙骗收件人的眼睛。

事实上，能认知世卫组织或疾病预防控制中心的准确 URL 的人并不多；因此可以推测，通过查看攻击者制造出类似的 URL 及邮箱地址，几乎没有人能发现或怀疑此为网络攻击。【图 1】中伪装成世卫组织电子邮件的发件人地址使用了“who.org”，但实际上世卫组织官方网站地址则是“who.int”。正常的网站地址反而给人一种比不正常的邮箱地址更假的感觉，这倒也并不奇怪。



【图1】伪装成世卫组织（WHO）电子邮件地址和主页地址



From: CDC-INFO <cdchan-00426@cdc-gov.org>
Sent: Friday, January 31, 2020
To:
Subject: 2019-nCoV: New cases around your City

Distributed via the CDC Health Alert Network
January 31, 2020
CDCHAN-00426

Dear

The Centers for Disease Control and Prevention (CDC) continues to closely monitor an outbreak of a 2019 novel coronavirus (2019-nCoV) in Wuhan City, Hubei Province, China that began in December 2019. CDC has established an Incident Management System to coordinate a domestic and international public health response.

Updated list of new cases around your city are available at
(https://www.cdc.gov/coronavirus/2019-nCoV/newcases-cities.html)

You are immediately advised to go through the cases above for safety hazard

Sincerely,
CDC-INFO National Contact Center
National Center for Health Marketing
Division of eHealth Marketing
Centers for Disease control and Prevention

【图2】 伪装成美国疾病预防控制中心（CDC）的电子邮件

2. 短信诈骗和电话诈骗

对个人携带的智能手机进行的短信攻击（Smishing Attack）和欺骗用户造成金钱损失的电话诈骗攻击（Voice Phishing Attack）正在持续增加。在春节、中秋、圣诞节等需要向熟人发送问候的时期或快递量剧增的时期，通过手机短信传播的手机恶意代码“短信诈骗”就会开始流行起来。

但如今随着生活方式的变化，网上购物已经不再局限于特殊时期，而是成为了日常生活中非常普遍的事；因此，收到告知配送情况的各种短信也是生活中很自然的事了。尤其，由于受到新冠病毒的影响，导致无法正常进行线下活动，因此网上配送需求量急剧增多，并在这一时期，以智能手机用户为目标的短信诈骗也随之增加。最简单方式，是伪装成快递配送短信，诱导用户访问的方式。过去的短信诈骗攻击组织主要通过使用短网址（URL）组成智能手机短信，将智能手机用户的怀疑降到最低，诱导用户访问 URL。如果按下短信的短网址，就会下载攻击者事先制作好的安卓智能手机应用程序的扩展名为 APK 的文件。虽然以前的方式是不经过安卓智能手机应用程序的正式流通窗口“谷歌 Play Store”，而直接诱导安装恶意 APK 文件。但从去年开始开展活跃活动的短信诈骗攻击组织，为了可以准确区分攻击对象，使其试图下载应用程序的方面上增加了逻辑性，表现出缜密的一面。他们首先确认访问者是通过智能手机还是电脑访问了自己制作的恶意应用程序下载页面。

然后进行第二次验证，确认是否是已掌握的智能手机号码后，让其下载恶意应用程序。这样做可以尽量避免其应用程序暴露在他们不情愿的地方。通过此过程，即使恶意应用程序下载 URL 被恶意代码分析专家或网络安全公司发现，打开的也不是攻击者制作的网络钓鱼页面，而是正常的快递公司网页，使其无法下载恶意 APK 文件，因此可以在不受任何干扰的情况下进行攻击。与常规的安卓智能手机应用程序相比，这种短信诈骗应用程序具有更多的权限。这表明了攻击者是想通过短信诈骗应用程序收集智能手机内部的用户信息的意图。

另外还确认到， 恶意利用韩国政府为有效克服新冠病毒而发放的“政府紧急灾难支援金”相关的内容，以“政府紧急灾难支援贷款向导”为托辞诈骗。冒充 KB 国民支援、友利金融支援等制度圈银行的商号或

冒充平民金融振兴院、国民幸福基金等公共机构的商品，诱导用户误认为是有公众信任机构发送的短信。而且还发现，通过“按先后顺序限量支付”、“限额即将耗尽”等刺激性的表达方式，利用那些需要紧急资金的人的不安心理进行诈骗的类型。为了避免遭受此类损害，我们应该了解利用短信和智能手机应用程序的恶意攻击。

3. 针对基础设施的网络攻击

网络攻击从未放弃过为在网络领域占据战略优势的努力。尤其，可以确认存在试图通过对国家主要基础设施的目标攻击来掌握基础设施的内部，并在以后可将其用于指定目的的攻击上。另外，还发现了一种鱼叉式网络钓鱼（Spear phishing）攻击，在这种攻击中，发件人姓名使用韩国特定组织的实际职员姓名，而收件人职位仅限制在相关职位的负责人，然后发送伪装成文档文件的带有恶意代码的附件。

由微软 Word 文档制作的这一恶意代码通过内部宏文件执行恶意操作。因此，在用户首次打开文档后，将弹出一个安全警告显示“是否运行宏指令”的选择菜单。在查看该组织的职员名单时，可以看出发件人确实是实际工作人员的名字。从这个例子中可以看出，攻击者很狡猾，他提前收集信息，以便在攻击中准确利用。当打开电子邮件附带的文档文件时，实际上真的会打开有关 2019 新型冠状病毒的内容，因此很难发现任何可疑之处，但此附件是攻击者精心准备的恶意文件，它会收集和泄露储存在用户电脑中的重要信息。

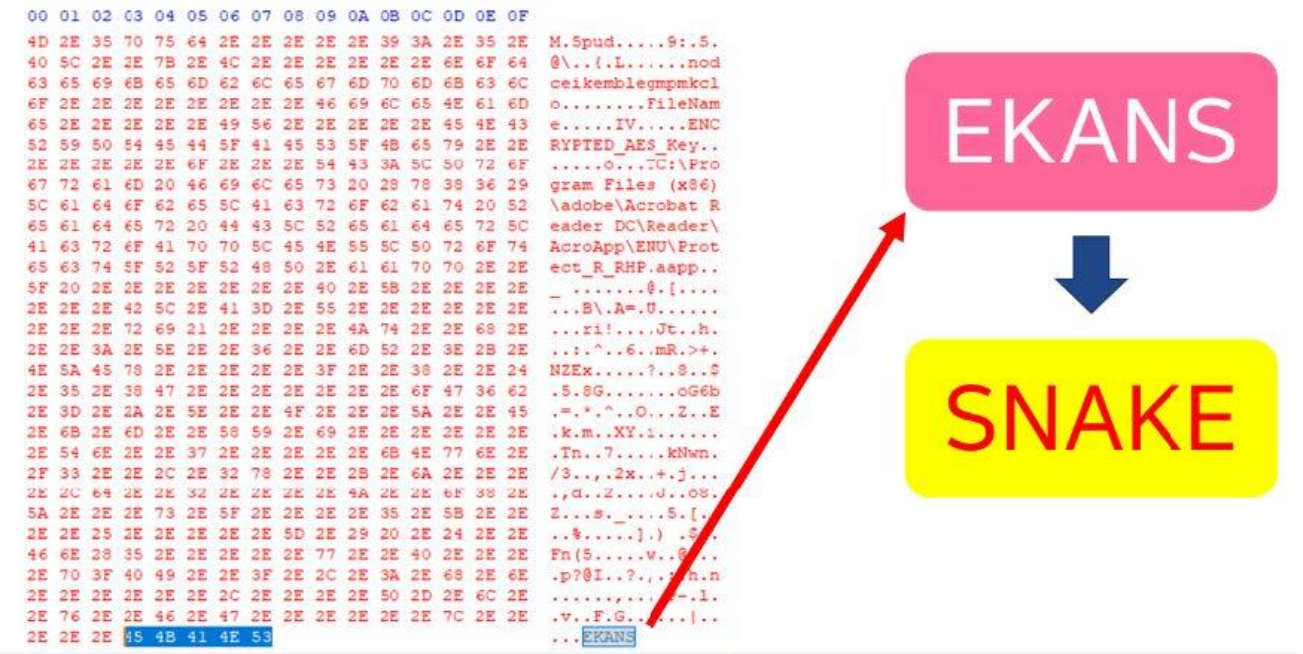
在韩国出现大规模 2019 新型冠状病毒确诊患者的时期，伪装成韩国“新天地”教会相关资料的文档文件引起了人们的注意，并诱导用户浏览文档。该文档包含两种内容，因此巧妙地避开了用户的怀疑。打开文档时，通过注册表项注册，在重新启动计算机后，攻击者所企图的后门程序仍会继续运行，并且传输进程列表、计算机名称、操作系统版本信息，还进行文件执行和终止、下载其他文件，以收集及泄露主要信息。另外，还确认了以介绍有关新型冠状病毒口罩的相关中国国内情况为内容的电子邮件流入韩国特定企业的事例。当解压压缩文件并运行，将安装并运行收集 NanoCore RAT（一种远程命令执行恶意代码，该恶意代码泄露 PC 内部主要信息）。NanoCore RAT 于 2013 年首次发现，具有类似于键盘记录器的各种功能，可以从 PC 收集数据并传送给攻击者。NanoCore RAT 可以远程打开或关闭 PC，运行文件，记录键盘的输入值，还可以锁定 PC，甚至可以通过网络摄像头进行录制。上述针对性攻击都是由国家主导的网络攻击集团及与其具有相同理念的组织进行的，特别是以韩国基础产业及军工企业为目标进行的攻击。

这些攻击集团旨在通过基本安全系统的崩溃来访问内部，控制基础设施以及并收集及泄露重要机密信息，最终目的是“泄露核心技术”和“通过侦察树立应对策略”。为了保护企业和组织安全免受针对韩国基础产业及军工企业的网络攻击的第一步，必须注意内部使用的电子邮件的附件。这是最基本、最重要的部分，因此即使多次强调也不容忽视。

4. 已渗透 OT 环境的勒索软件

尽管勒索软件（Ransomware）埋没在众多 IT 安全事件和事故中，但它仍然是主要的安全威胁。其中，还必须注意针对工控系统的勒索软件攻击。2019 年 3 月，LockerGoga 攻击了欧洲的制造公司，将文件

加密以导致生产线停止运行，它具有 5 个主要特征：▲仅加密 30 个扩展名，▲使用安全的电子邮件，▲使用有效的数字签名，▲通过协商调整支付金额，▲收集组织内部信息并将其泄露。



【图 3】针对工控系统的Snake勒索软件

今年初值得关注的勒索软件是 Snake。Snake 勒索软件使用 Go 语言，用勒索软件加密的文件内部的最后部分添加了“EKANS”的字符串等，显示出了自己固有的特征。Snake 勒索软件是典型的针对工业控制系统的勒索软件，主要攻击控制系统的操作系统基于 Windows 的各种生产设备。

除了勒索软件，各种目的的恶意代码也用于对工业控制系统的针对性攻击，并且攻击范围正在逐渐扩大。一旦被感染，具有致命打击的勒索软件的攻击已渗透到 OT 环境，构建和管理工业控制系统的安全系统比以往任何时候都更为重要。

5. 网络摄像头勒索

与性敲诈相关的安全威胁的典型的手段是“网络摄像头勒索”。网络摄像头勒索是指攻击者欺骗对方通过视频聊天诱使对方性行为并将其记录下来，然后勒索对方“将视频释放给熟人”并索要金钱的一种勒索方式。
在此过程中，攻击者诱使受害者安装恶意应用程序以窃取受害者的智能手机上的通讯录信息。如果受害者被诱骗安装恶意应用程序，攻击者将窃取存储在智能手机上的通讯录、短信等信息。

最近，随着远程视频会议的活跃使用，从 2000 年代中期开始逐渐消失的网络摄像头又重新登场，由此引发的性勒索威胁的发生可能性会变得更大，因此须对此做好应对准备。如果收到带有网络摄像头勒索形式内容的电子邮件，不要感到惊讶或紧张，不管是什么内容，删除后就不要放在心上才是至关重要。如果还是觉得担心，就先删除电子邮件，并根据需要，考虑一下删除正在使用的账户，更换密码，退出服务会员等。如果在邮件标题中有自己使用的密码时，请重新确认自己目前的个人信息状态，并建议废弃同一密

码。这是云服务开始被广受利用后特别要注意的地方。此外，因为所有网络服务都可以通过 Facebook、Naver、Kakaotalk、Twitter 等账号登录，因此需要格外注意。要严格管理网上或智能手机使用的 ID 和密码，如果怀疑个人信息被外泄时，请立即将自己使用的密码换成其他密码，以防止攻击者执行进一步攻击。

到目前为止，2020 年上半年出现了 5 种网络安全威胁，分别是：▲恶意利用新冠病毒的网络安全威胁剧增，▲短信诈骗和电话诈骗的增加，▲基础设施为目标的恶意代码，▲渗透到 OT 及 ICS 领域的勒索软件，▲网络摄像头勒索。

安全威胁会恶意利用各种社会焦点问题，因此应该注意政府机构及安全公司提供的各种形态的威胁信息。同时，希望通过摸索符合自身公司业务环境的对策，在更加安全、自由的网络环境中开展业务。

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
© 2020 AhnLab, Inc. All rights reserved.