你的个人信息安全吗？

通过韩剧《幽灵》了解网络威胁在现实生活中的可能性

我们的生活越来越离不开智能手机、平板电脑、互联网、微博、邮件等，人和人之间的距离越来越近，也越来越远。公车和地铁上，大多数的人在埋头玩自己的手机。随着网络的发展，我们随时随地可以连接到互联网。你有没有想过自己的一举一动可能随时被互联网里的“幽灵”监控？苏志燮主演的韩剧《幽灵》就是讲述了网络刑警侦破高科技犯罪的故事。

《幽灵》作为一步以网络犯罪为题材的韩剧，剧中使用了大量黑客入侵电脑技术。很多电视剧观众对剧中的安全技术表示极大的兴趣，更是受到大家的热议，连不少网络安全领域的专业人士也非常着迷追剧。PPS 网络电视上的评分高达 9.4，可以看出《幽灵》在中国大陆很有人气。

人们也好奇，剧中的黑客入侵技术在现实生活中真的可以发生？对此，本刊对该剧中出现的网络攻击技术中，最有可能威胁到现实世界的几部故事为中心讲述，提醒人们使用互联网的时候要提高警惕，并关注保护个人隐私。

利用电子邮件传播恶意代码

剧中数次登场通过电子邮件附件感染对方电脑的恶意代码传播方式。通常病毒感染是通过不特定多数对象传播，而剧中是针对特定对象传播，称为针对性攻击（Targeted attack）或者钓鱼攻击（Spear Phishing）。这种攻击预先选定攻击对象，再配合社会工程学实施的邮件欺骗攻击。

实际使用在针对性攻击的邮件附件大部分是伪造的文档文件，并不是可执行文件。当收件人打开文档时，利用漏洞感染用户电脑，用户全然不知。

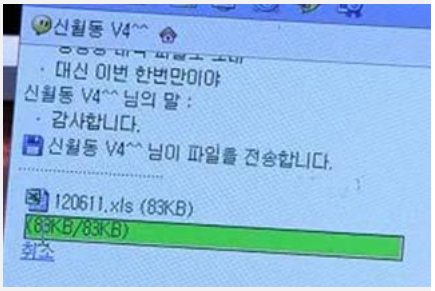
通过邮件附件感染恶意代码是经常使用的一种攻击方法，因此现实可发生的危险极高。用户在打开来历不明的邮件附件的时候一定要谨慎，如果怀疑是病毒文件，请立即删除。

韩剧《幽灵》简介

《幽灵》为 2012 年 5 月末开始在韩国 SBS 电视台播放的电视剧。该剧由当红影星苏志燮和李妍熙主演，以网络犯罪和网络刑警为题材。讲述了随着社交网络的发展而产生的新型犯罪和与这些犯罪做斗争的网络刑警们的故事。

虽然是虚构，但是由韩国顶级综合网络安全公司-AhnLab 提供技术咨询，并直接到 Ahnlab 公司现场拍摄，追求更高的真实性。

剧中经常出现的监控中心正是 AhnLab 公司的 SOC（Security Operation Center）室。不仅提供了各种网络安全和黑客技术的咨询，还提供了外景拍摄，AhnLab 公司为这部剧的完成度做出了极大的贡献。



【图-1】文档里隐藏恶意代码传送

AhnLab 监控中心 SOC

剧中经常登场的黑客行为和远程监控的场景是在 AhnLab 公司的 SOC(Security Operation Center)室拍摄的。
SOC 室的一个墙面全部共由 18 台的平面显示屏构成，安全专家时刻监控客户的网络现状并做出及时响应。

【图-2】Ahnlab SOC 室

利用未知程序漏洞的零日攻击

剧中，哈迪斯利用 MSN 连线聊天和传输 Excel 文件，顺利地拍到黑客的图片，虽然只是一张图，但对破案有着关键作用。哈迪斯是怎样做到的呢？首先利用 Excel 程序的未知漏洞在文档里隐藏恶意代码，当对方打开 Excel 文档时，恶意代码将隐秘地运行电脑视频程序，开始传送图片。这样的利用未知漏洞的攻击称为零日攻击（Zero-day attack）。在安全漏洞补丁程序还未发布之前，阻止零日攻击的方法并不多。最近，入侵企业内部截取重要情报并破坏系统的高级持续性威胁（APT：Advanced Persistent Threat）主要利用这样的攻击方法。

虽然零日攻击不是很普遍发生，但是一年有几次是在实际攻击中使用，现实危险还是存在的。因此为了保护系统，必须安装安全软件并经常更新安全漏洞补丁。

利用远程漏洞的攻击

通常的网络攻击是按扫描(Scanning) → 向服务端口传送攻击代码 → 系统权限上升(攻击成功)的顺序进行。

攻击出发点“扫描”是确认网络运行的主机的工作程序，或是为了对主机进行攻击，或是为了网络安全评估。扫描是攻击者情报搜集的 3 个组成部分之一。在足迹打印阶段，攻击者创建一个目标组织的轮廓，包含一些信息例如它的域名系统（DNS），电子邮件服务器，还有 IP 地址范围。这些信息中大部分可以在线得到。在扫描阶段，攻击者找到了关于特定 IP 地址的信息，该 IP 地址可以通过因特网进行评估，如他们的操作系统、系统结构和每台计算机上的服务等情况。在列举阶段，攻击者搜集关于网络用户、工作组名称、路由表和简单网络管理协议等资料。

服务端口可以说是系统运行的程序与外部数据通信的通道。通常被称为 Exploit 的攻击代码利用系统或者应用程序的安全漏洞，按照攻击者的意图下恶意指令。

攻击者确认服务端口或与此相关的守护程序后，要具备适当的攻击方式。可以使用众所周知的攻击手段，也可使用未知的、无法阻挡且自己开发的攻击手段。传播在网上的恶意代码或黑客工具是第一种攻击手段，利用未知漏洞的零日攻击(Zero-day attack)则是第二种攻击手段。

DDoS 攻击和僵尸电脑

DDoS（Distributed Denial of Service），即分布式拒绝服务是使用多台 PC 同时访问特定的网站，服务器超负荷，从而使服务器无法处理合法用户指令。DDoS 攻击的成功在于确保了多少僵尸电脑。僵尸电脑是指接入互联网的计算机被病毒感染后，受控于黑客，可以随时按照黑客的指令展开拒绝服务（Dos）攻击或发送垃圾信息。

剧中，通过文件共享网站在发布的视频文件里隐藏恶意代码，以此感染多台电脑。实际攻击者为确保多数僵尸电脑，而采取的方法如下：

1. 入侵众所周知的网站，利用为恶意代码发布地；
2. 入侵众所周知的应用程序更新服务器，利用为恶意代码发布地；
3. 在文件共享网站（P2P），上传引起人们兴趣的视频文件等，发布恶意代码。

通过无线局域网(WLAN)窃取个人信息

智能手机在这几年中取得了突飞猛进的发展，这种发展趋势还在延续。据工信部电信研究所最新发布的数据显示，今年 4 月，中国智能手机出货量为 1811.4 万部，市场占有率过半。随着智能手机、平板电脑等各类智能终端的普及率越来越高，对无线网普及的需求也越来越高。

剧中，我们看到智能手机发送的短信可能被窃取。越来越多的餐饮、休闲娱乐场所都会提供免费 WiFi，不少人不假思索地使用搜到的免费账号登录上网的同时，却不知个人信息安全已经遭遇到了威胁。在公共地方使用免费 WiFi 并不安全，通过 wifi 可以窃取个人信息。这让不少习惯用 WiFi 上网的用户们开始担忧。

为防止个人信息被黑客窃取，我们建议以下安全守则：

1. 使用无限网路由器的时候，设置安全功能；
2. 安全管理无线网路由器的密码；
3. 不使用无线网时，关闭路由器；
4. 不使用提供者不明确的无线网；
5. 通过没有设置安全功能的无线网不使用敏感的服务；
6. 禁用无线网自动连接功能；
7. 更改无线网路由器的名称（SSID），并设置为隐藏。

关键基础设施攻击的现实可能性

在《幽灵》中，最为引起人们争论的故事情节为电力系统被黑客攻击，从而导致大规模的停电事故。该事故的起因为电力公司安全部门的职员的 U 盘被人动手脚，通过该 U 盘感染了整个电力系统。虽然是虚构的，但是让人看得心惊胆战。如果在现实世界发生了这样的情况，它的传播效应是不可想象的，可能比电视剧更为严重。

实际上，该主题是从几年前在伊朗核电站发生的被 Stuxnet 攻击事件取材的。Stuxnet 的持久性和复杂程度震惊了全世界，特别是安全行业。这种有针对性工业控制系统编写的破坏性病毒让那些相信封闭式的网络在某种程度上不会受到外部攻击的所有类型系统的运营者瞠目结舌。

像电力系统之类的社会基础设施没有连接到外部互联网，它在封闭式的网络中运营。在封闭式的网络，外部的恶意代码可以入侵到内部的唯一途径是 U 盘之类的存储式移动装置。当 U 盘插入电脑的瞬间，恶意代码将被 U 盘的 AotoRun 功能自动运行，从而感染电脑主机。

但是，利用 U 盘感染目标的恶意代码不限于 Stuxnet 一个种类。已经有数多的恶意代码采用了通过 U 盘自动运行功能感染的方式，因此格外注意 U 盘的安全使用。

【图-3】通过 U 盘感染系统

Stuxnet 和 SCADA 系统

Stuxnet 蠕虫病毒是 2010 年发现的世界上首个专门针对工业系统编写的破坏性病毒，能够利用对 windows 系统和西门子 SIMATIC WinCC 系统的 7 个漏洞进行攻击。特别是针对西门子公司的 SIMATIC WinCC 监控与数据采集（SCADA）系统进行攻击，由于该系统在多个重要行业应用广泛，被用来进行钢铁、电力、能源、化工等重要行业的人机交互与监控。传播途径：该病毒主要通过 U 盘和局域网进行传播。

【图-4】安博士公司楼

结束语

近年来，随着网上金融交易和网上购物等互联网应用的兴起，个人隐私信息变成了网络中流动的数据，非法收集、利用、公开个人信息的机会之门也由此大开。随着个人隐私信息的泄漏，各种敲响网络安全警钟的事件也陆续发生。去年年底，中国互联网遭遇了史上最大规模的用户信息泄漏事件，几千万用户账号和密码被公开，个人信息保护问题被推向舆论的风口浪尖。

剧中的故事情节几乎都是实际在网络发生的事件为素材改编的。尤其是剧中运用的黑客工具和反黑工具、以及黑客攻击的安全漏洞都比较真实。

《幽灵》播放以来受到了人们的好评，大家纷纷表示新鲜和惊讶，因为这是在韩国首次以网络犯罪为题材的电视剧。电视剧的传播效应确实很大，对网络安全一无所知或者略知的人也开始关注个人隐私泄漏的问题。

安博士希望通过电视剧《幽灵》，能够告诫人们网络有很多威胁存在，需要人们在使用互联网时提高警惕。