AhnLab

安全月刊

2015.06 Vol. 32

上半年恶意软件趋势

2015上半年恶意软件趋势

主要关键词是“变种”…
变种恶意软件的出现

2015年上半年，有关恶意软件的主要特征可以说是现存恶意软件再次出现新变种。如同“阳光底下本无新事(There is Nothing New under the sun)”，同样的恶意软件往复再现，不同的只是应用了新的攻击手法。即使是已知的恶意软件，加上一点点变形的手法，便成为变种恶意软件。因此，防御起来也不容易。这种恶意软件有“勒索软件(Ransomware)”、“利用垃圾邮件的 Upatre”、“SCR(Screensaver)恶意软件”和“宏病毒”等。

本刊将重点介绍2015上半年主要恶意软件攻击事例和其预防方法。

人人惧怕的“勒索软件”

2015年上半年，成为韩国最大话题的恶意软件是“勒索软件”。在国外，勒索软件从2013年开始受到注目，已流行多年。去年，在韩国首次被报告PC被勒索软件感染事件发生之后，最近陆续发生了企业和机关发生了被勒索软件感染事件。尤其是今年4月，通过社区网站传播 CryptoLocker 勒索软件事件发生之后，勒索软件的危害性便浮出了水面。

代表性的勒索软件如下：

- **SimpleLocker**：移动勒索软件的一种，将智能手机中的图片、视频和文档加密后索要赎金。从2014年5月开始不断地出现。
- **CryptoLocker**：将用户计算机中的文件加密后，索要比特币或现金，如果用户不支付“赎金”，文件将会被永久加密。
- **Scareware**：该勒索软件是最简单形式的恶意软件，伪装成假杀毒软件或清除病毒工具，向用户告知他们的计算机感染了病毒，诱使用户下载恶意软件。
- **Lock-Screen**：如果被该勒索软件感染，则完全无法使用计算机。通常打开几个全屏大小的Windows窗口，上面还刻有 FBI 或司法部的标记，警告用户非法下载等违反法律，需要交罚款。

其中，勒索软件 CryptoLocker 主要是利用用户系统漏洞的通过基于 Web 的 DBD(Drive-By-Download)方式感染的。当用户访问有名的社区网站，即重定向到具有漏洞的网站，同时下载勒索软件并安装到用户的计算机。

通常，勒索软件感染用户计算机之后，即在桌面显示勒索信息，并将计算机上的私人文档和图片等加密导致无法打开。如果用户不支付赎金，文件将可能永久无法解密。在韩国发生的勒索软件，以韩文显示勒索信息并向用户索要438,900韩元的比特币。为了使受害用户容易支付赎金，详细描述了付款方法。还免费对一个文件解密，证明拿到赎金后他们会即刻恢复所有文件。

陆续发生的韩文版勒索软件事件，已证明韩国已不再是勒索软件的安全地带。勒索软件之所以成为人人惧怕的对象，是因为持续出现变种的勒索软件。实际在出现韩文版勒索软件以后，出现了具备 DDos 攻击功能的勒索软件，引起大量网络流量使网络瘫痪。另外，一旦被勒索软件感染，即使支付了赎金，也不能保证文件完好无损。这也是勒索软件成为畏惧对象的一个原因。除此之外，还出现了针对移动设备的勒索软件和瞄准玩家金币的勒索软件等，勒索手法越来越精巧，用户要格外注意。

要防止被勒索软件感染，重要的是事前预防。最近被报告的勒索软件感染路径中，最多是利用垃圾邮件感染。因此，不要随意打开来源不明，尤其是扩展名为 ZIP 或 RAR 的电子邮件附件。即使是来源明确，但怀疑是垃圾邮件的话，请不要打开附件并立即删除。还要做到经常备份重要文件，并将备份文件保存到移动式存储设备或云中创建网盘后保存。

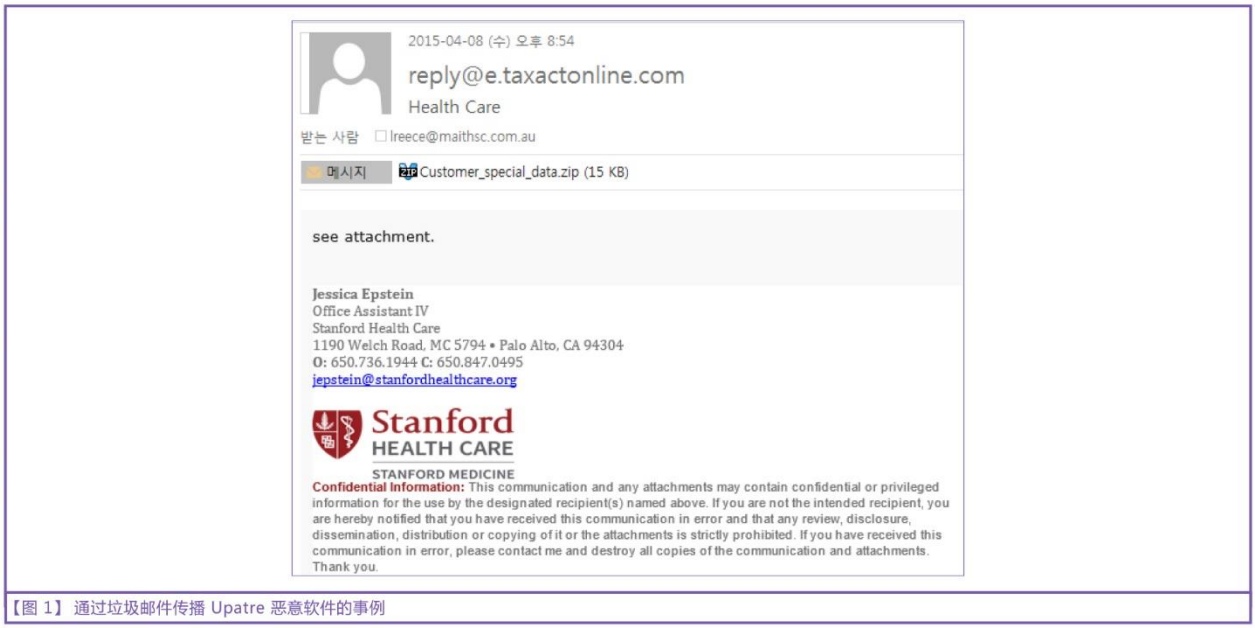
重要文件的属性设置为“只读”也有助于防御勒索软件。大部分的勒索软件加密时需要更改文件，因此重要文件进行更改后将属性更改为“只读”的话，可以阻止勒索软件对该文件的加密。

最后，积极更新您的防病毒软件和操作系统等守好基本的安全守则，也有助于防止被勒索软件感染。

通过垃圾邮件传播的 Upatre 恶意软件

如前面所述的勒索软件可以看出，目前全世界最有效的恶意软件感染路径是通过垃圾邮件伪装成附件进行传播。这些垃圾邮件利用社会工程学引诱用户点击邮件文本中的链接或者打开并执行伪装成附件的恶意软件从而导致被感染。在韩国，从去年后半年开始到今年上半年，持续出现大量的伪装成附件的 Upatre 恶意软件。国外早在2013年8月开始就出现了该恶意软件，并呈现持续增长。

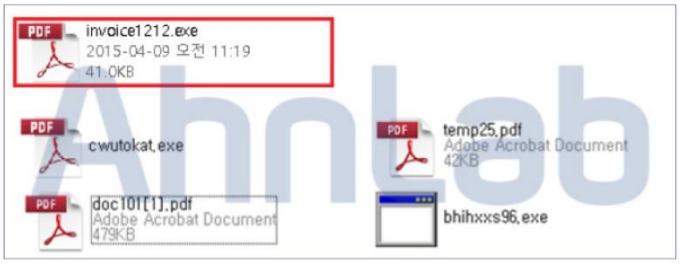
Upatre 恶意软件根据其变种会有些差异，但是共同执行如下的动作。▲ 运行垃圾邮件中的附件时创建副本 ▲ 试图访问 C&C 服务器并下载恶意软件 ▲ 运行正常 PDF 文档伪装成正常的文件 ▲ 持续与 C&C 服务器通信并盗取重要信息



【图 1】 通过垃圾邮件传播 Upatre 恶意软件的事例

包含该 Upatre 恶意软件的垃圾邮件的标题和文本内容主要使用 doc, document, invoice, ticket, photo 等单词引诱用户点击。

最近，AhnLab 收集的 Upatre 变种通过标题为“invoice”的垃圾邮件传播。如【图 2】所示，邮件的附件伪装成 PDF 文件，实际是可执行文件“invoice1212.exe”。



【图 2】垃圾邮件附件‘Dropper’及创建的文件（invoice121.exe 以外的4个）

当用户点击下载并运行“invoice1212.exe”，则生成一个新的文件，该文件试图连接 C&C 服务器并下载恶意软件到用户计算机。值得注意的是，该恶意软件为了掩饰这些事情，在运行“invoice1212.exe”的同时打开一个正常的 PDF 文件，隐藏恶意行为使用户蒙在鼓里，全然不知被感染。这种恶意软件大部分具有间谍软件功能(Infostealer)，会偷取计算机内寄存的个人信息，并将这些信息传递到黑客指定的电子邮件。

目前 Upatre 恶意软件的变种持续出现。为了预防这些变种的 Upatre 恶意软件，在打开电子邮件时注意是否包含了上面所述的经常出现在垃圾邮件的单词。或者，将这些单词登记为过滤关键词，分类到垃圾邮件，最好即刻删除。另外，不要轻易打开来源不明的电子邮件，最好也即刻删除。

伪装成 SCR(屏保)程序的恶意软件的威胁也在进行中

如果在使用计算机进行工作的过程中临时有一段时间需要做一些其他的事情，从而中断了对计算机的操作，这时就可以启动屏幕保护程序，将屏幕上正在进行的工作状况画面隐藏起来。[1] SCR(Screensaver)是屏幕保护程序的扩展名。大多数的计算机用户对于 SCR 扩展名可能有点生疏，但必须要知道 SCR 扩展名也可以用在恶意文件。因此，在下载屏保程序时需要格外注意。

【表 1】列出了 AhnLab 发现的恶意 SCR 文件中的一部分。可以看出，从去年开始到今年上半年持续出现了 SCR 恶意软件。这些文件只不过是 AhnLab 收集到的部分样本，实际种类很多。

收集日	文件名	图片描述
2014年 4月	1.scr	密码更改向导
	2.scr	登录向导
2014年 5月	.scr	访问向导
2014年 9月	목장.scr	牧场
	안면도.scr	安眠岛
	추석인사.scr	中秋节问候
	수목원.scr	树木园
2014年 10月	김정은결석.scr	北朝鲜人民大会图片
2014年 11月	포스터.scr	创作大赛
2014年 12月	2015새해인사.scr	新年问候
	좋은글 연하장(1).scr	新年贺卡
2014年 1月	가슴1.scr	淫乱图片
	연구결과.scr	统计资料
	대중 세미나.scr	研讨会资料
	방문투표관련공고.scr	有关住宅小区的选举
	통장사본.scr	存折副本
2015年 3月	001.scr	宣传
	002.scr	机票促销活动
	스트림.scr	山谷的风景照
	안보의식조사서.scr	安保意识调查书
2015年 4月	1.scr	车模照片
	2.scr	车模照片
	3.scr	车模照片
	겉표지.scr	图书封面
	목차.scr	图书目录

【表 1】扩展名为 SCR 的恶意软件

从表中我们还可以看到，实际打开后的图片有“新年贺卡”、“车模照片”等，还有“北朝鲜人民大会”有关照片、“统计资料”和“国民安保意识调查报告”等有关政治的内容。这些文件都具有表示图片的图标。当文件被运行时，嵌入在文件内部的广告或文件截图等图片文件也将被运行。该文件在C盘的特定路径创建PE文件，接着盗取用户信息。

[1] 百度百科

如果这种文件传到国家重要机关或企业，有可能泄漏重要的信息。这种攻击从过去到现在持续出现，要特别注意。

宏病毒的重现

宏病毒是一种寄存在文档或模板的宏中的计算机病毒。一旦打开这样的文档，其中的宏就会被执行，于是宏病毒就会被激活，转移到计算机上，并驻留在Normal模板上。从此以后，所有自动保存的文档都会“感染”上这种宏病毒，而且如果其他用户打开了感染病毒的文档，宏病毒又会转移到他的计算机上。[2]

宏病毒最早出现于1995年，针对 Office 用户广泛传播，到2000年初几乎消失。但惊讶的是，2014年又重新出现并逐步增加，到今年几乎每天发现1~2个新的宏病毒。2015年3月，媒体也纷纷报道“宏病毒起死回生”。

【图 3】有关 Office 恶意软件增加的新闻

AhnLab 收集到的宏病毒数如【表 2】所示。从表中我们可以看到，2015年5月为止收集到的宏病毒数远远超过了去年一年收集到的宏病毒数。

年度	收集数量
2012年	22个
2013年	50个
2014年	108个
2015年 1~5月	387个

【表 2】AhnLab 收集到的宏病毒数量统计

攻击者通常将病毒伪装成简历表、订单等文档后，通过电子邮件附件发送，诱使用户点击附件并打开。到目前为止，大部分的垃圾邮件的语言是英文。偶尔会有欧洲地区语言发送的邮件和附件。Microsoft Word 几乎已经成为全世界办公文档的事实工业标准。在韩国宏病毒主要围绕在与海外交流频繁的企业为中心发生。因为韩国的个人计算机用户很多使用 Hangul 文字处理软件，因此相对来说个人用户的受害较少一些。

由于宏病毒的经常出现，Office 默认将宏设置为禁用。但是，最近出现的宏病毒利用社会工程学手法诱使用户启用宏功能。最为常用的方法是在打开文档时会提示用户启用宏功能才可以打开文档。如果启用宏功能，屏幕没有任何变化而病毒已在运行。有些病毒在运行时，给出其他的内容而欺骗用户，这主要发生在Excel文档。

攻击者利用宏病毒可以下载或生成其他病毒。宏病毒主要危害如下：▲ 泄漏用户信息 ▲ 盗取金融信息 ▲ 远程控制等。宏病毒隐蔽性强、传播迅速、危害严重，难以防治。因此，在打开电子邮件附件收到的文档时要谨慎，切记要将 office 宏功能设置为禁用。

[2] 百度百科

http:// cn.ahnlab.com

http://global.ahnlab.com

http://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） | sales@ahn.com.cn