AhnLab

安全月刊

2017.10 Vol. 59

Threat Landscape

在勒索软件风暴中被遗忘的

与生活密切相关的安全威胁 Top 3

回顾2017年，世界被强大的勒索软件，如WannaCryptor和Petya所震撼。但是，在这危机的时刻，并不能忽视的与生活密切相关的安全威胁不断出现。本刊将回顾一下这种威胁的特点和事例，并希望读者们在每一瞬间都要注意这些安全威胁。

与生活密切相关的安全威胁之一，网络钓鱼

网络钓鱼（Phishing，与钓鱼的英语fishing发音相近，又名钓鱼法或钓鱼式攻击）是通过大量发送声称来自于银行或其他知名机构的欺骗性垃圾邮件，意图引诱收信人给出敏感信息（如用户名、口令、帐号 ID 、ATM PIN 码或信用卡详细信息）的一种攻击方式。最典型的网络钓鱼攻击将收信人引诱到一个通过精心设计与目标组织的网站非常相似的钓鱼网站上，并获取收信人在此网站上输入的个人敏感信息，通常这个攻击过程不会让受害者警觉。它是“社会工程攻击”的一种形式。网络钓鱼是一种在线身份盗窃方式。（来源：百度百科）

网络钓鱼是不容忽视的安全威胁之一，因为它针对不特定对象进行攻击并获取个人信息。获取的个人信息很有可能恶意利用在其他大量攻击，还会对泄漏个人信息的用户造成金融损失和有可能无意中被牵连到网络攻击。

目标系统(OS)	适用于PC和移动设备
主要行为	收集Web服务ID，密码和其他个人信息
其他特点	收集的信息恶意利用在其他网络犯罪
预防方法	检查登录时是否有特异事项
AhnLab解决方案	V3(阻止钓鱼网站功能)

【表 1】网络钓鱼的主要特点和响应方法

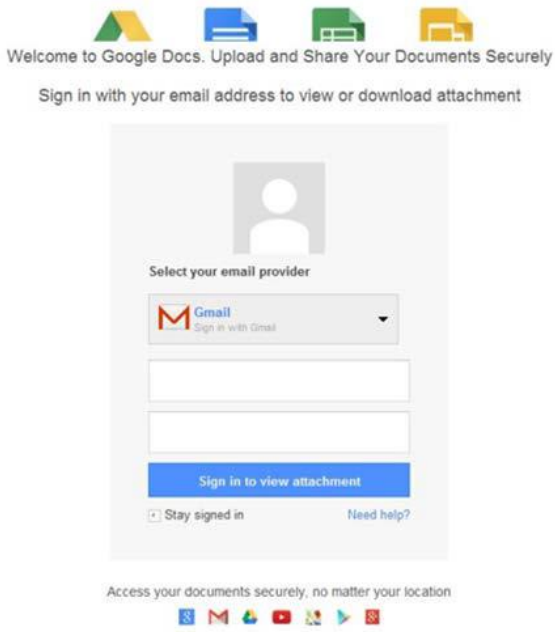
网络钓鱼攻击的主要事例

■ 伪装成Google云端硬盘的网络钓鱼邮件

攻击者将URL包含在电子邮件附件的内容中，然后引诱用户点击URL链接来访问网络钓鱼网页。

【图 1】伪装成PDF文件下载的网络钓鱼

点击【图 1】中的“下载”链接将转到Google云端硬盘登录界面，如【图 2】所示。Google云端硬盘是用于存储照片和文档的免费云端存储服务，Google文档是由Google云端硬盘提供的文档编辑功能。

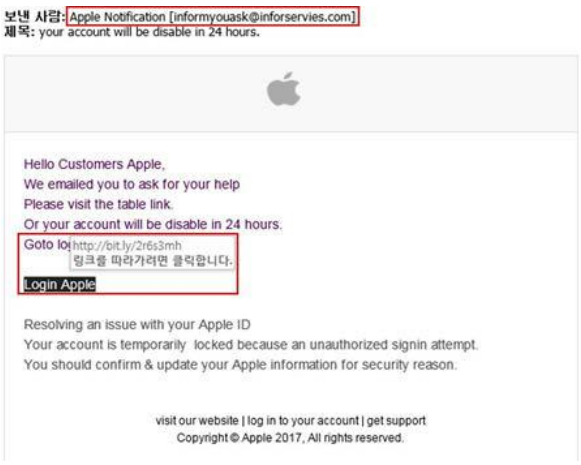


【图 2】伪装成Google文档的网络钓鱼网页

输入电子邮件地址和密码以打开附件，点击“登录查看附件”按钮，将帐户信息发送给攻击者提前设置的特定服务器。然后重新连接到正常的Google文档服务页面，使用户误认为使用正常的服务。如果您选择Gmail帐户作为您的电子邮件帐户服务，则需要其他手机号码或辅助电子邮件地址信息来恢复Gmail帐户。当用户输入附加信息时，收集该信息并传送给攻击者。

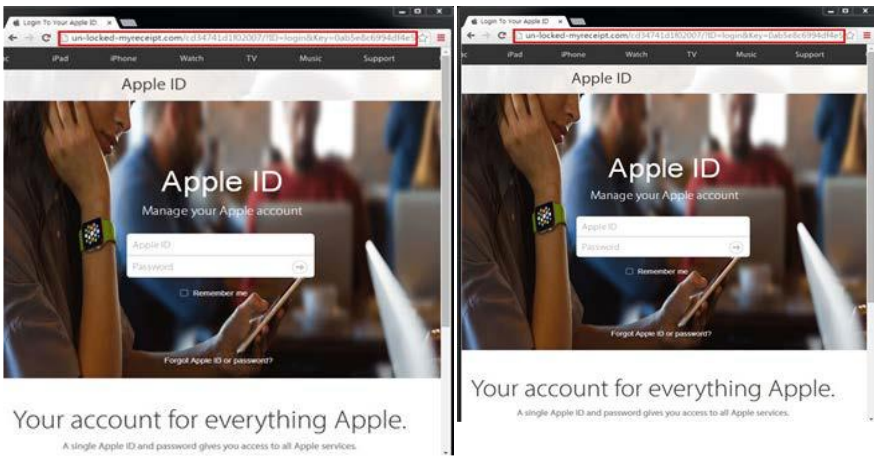
■ 伪装成苹果（Apple）服务的网络钓鱼邮件

攻击者伪装成苹果官网（Apple.com）发送电子邮件，邮件内容包含了用户的Apple帐户将在24小时内被禁用的内容，引诱用户访问网络钓鱼页面，如【图 3】所示。



【图 3】伪装成苹果服务的网络钓鱼

作为参考，Apple电子邮件通常使用apple.com域。点击网络钓鱼邮件中包含的缩略URL将访问与正常Apple主页设计相似的假网站。但是，如【图 4】所示，将网络钓鱼网站与正常Apple网站进行比较，看起来相同，但URL和安全协议略有不同。



【图 4】网络钓鱼网站（左）和苹果正常网站（右）

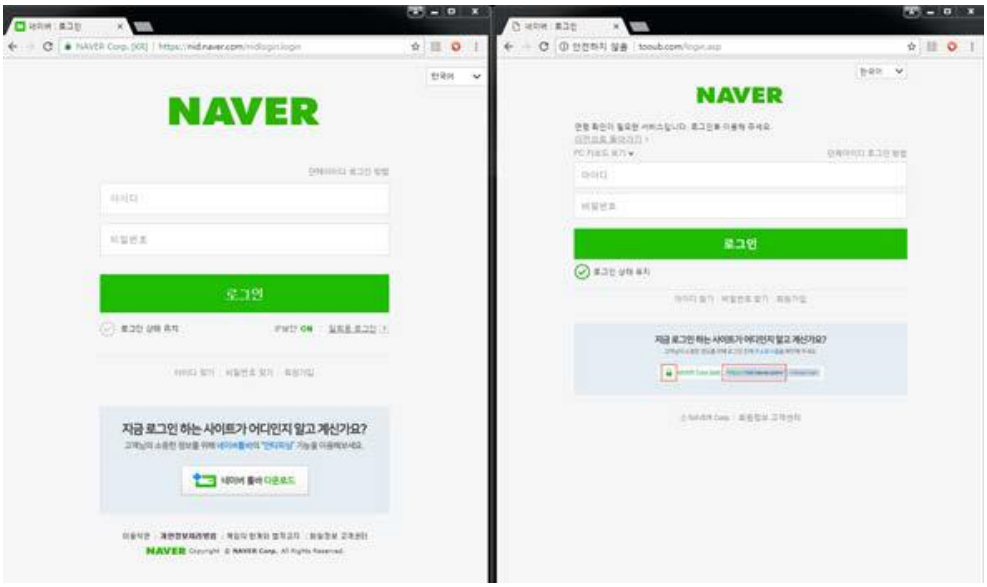
当用户通过点击缩略的URL打开的网络钓鱼网站中输入ID和密码时，提示用户“缺少验证用户ID所需的一些信息”的虚假信息，并引诱用户输入金融信息和个人信息以解决问题。通过此过程收集和传送的信息是：金融卡信息（卡号，CVC号码，到期日），个人信息（姓名，国籍，地址，邮政编码，出生日期，手机号码）等。

【图 5】收集信息后访问苹果正常站点

在输入完用户的个人信息后，激活输入信用卡相关的安全码的窗口，引诱用户输入安全码。一旦所有这一切过程都完成，它被重定向到一个正常的苹果网站，使用户误认为是正常的服务。

■ 通过社区网站帖子进行网络钓鱼

攻击者将带有刺激性的标题的帖子发表在知名社区网站，诱导会员的点击，然后通过网络钓鱼页面窃取个人信息。当用户点击帖子内容中包含的URL时，将连接到伪装成视频播放器的网页。如果点击页面上的视频播放器图标，它会将显示韩国着名的门户网站，并提示您输入帐户信息。



【图 6】韩国有名的门户网站登录页面（左）和网络钓鱼页面（右）

通过网络钓鱼页面收集的门户网站ID和密码将被发送给攻击者，之后始终播放与帖子的内容无关的视频。

■ 通过虚拟货币交易所的提示信息进行网络钓鱼

攻击者通过伪装成虚拟货币交易所的各种提示信息，如登录提示、购买提示、提款提示等来窃取虚拟货币交易所需的个人信息。攻击者通过诱导用户点击“立即开始”或“做交易”的按钮，或者通过屏幕上显示的URL与实际连接的URL不同的方式来欺骗用户访问网络钓鱼网站，并使用户输入个人信息。与此相关，各虚拟货币交易网站已经通知客户格外注意，但类似的攻击将在未来还将持续。

与生活密切相关的安全威胁之二，域欺骗

Pharming是网络钓鱼（Phishing）和耕作（Farming）的组合，即使用户在网络浏览器中输入正确的网站地址，根据由恶意软件篡改的hosts文件或DNS地址来诱导用户访问攻击者制作的假网站，并窃取有关在线金融交易的个人信息。大多数用户没有意识到被恶意代码感染，因为它们大多数是通过网页浏览器的收藏夹或直接输入正确的网址来访问网站。收集的用户信息包括门户网站服务的用户ID和密码，以及与在线金融服务相关的各种个人信息。另外，泄露的信息不仅被转售，还可能会导致个人的金融损失。我们必须认识到攻击者在这一刻也在为获取金钱利益而尝试着各种攻击，因此，用户在利用在线服务时特别要注意。

主要恶意软件诊断名	Trojan/Win32.Banki，Dropper/Win32.Banki 等
类型	银行业务（收集网上银行用户信息的目的）
目标系统(OS)	Windows
主要行为	收集在线金融服务ID，密码，授权证书，信用卡号，安全码
其他特点	导致直接的金融损失
预防方法	- 将V3更新到最新版本后，启用实时监控 - 引诱输入过多的个人信息时，怀疑服务异常
AhnLab解决方案	V3, MDS(恶意代码诊断•删除)

【表 2】域欺骗的主要特点和响应方法

域欺骗攻击的主要事例

■ 利用正常的实用程序的更新服务器分发恶意代码

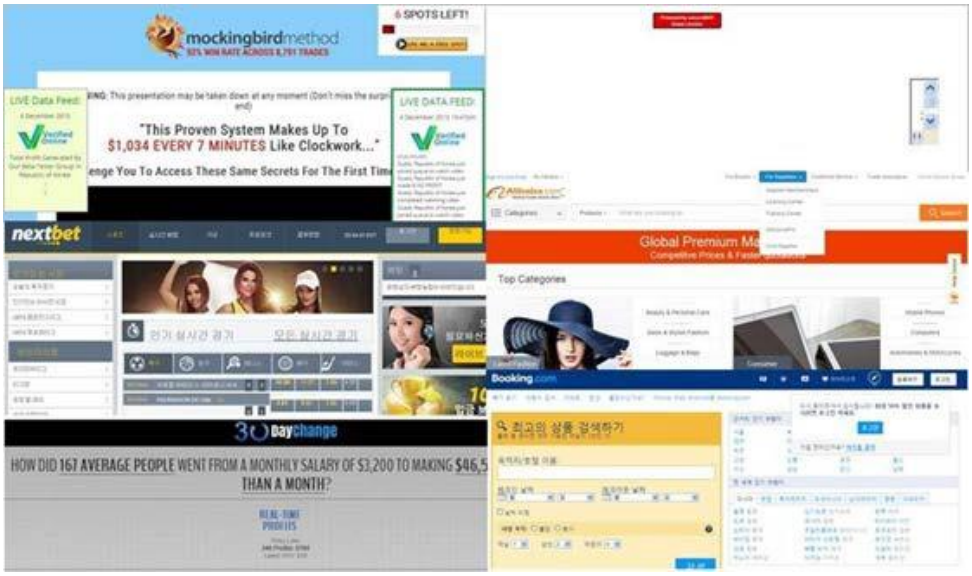
在域欺骗攻击中，发现了恶意利用正常实用程序更新过程的攻击事例。恶意文件从正常的更新路径中传播，文件运行后会创建文件并在注册表中注册，以便Windows启动时自动运行。此时生成的“[随机字符串].exe”文件会定期尝试连接到C＆C服务器以下载额外的文件。域欺骗行为通过下载的额外的文件执行，并将MAC地址发送给攻击者。

■ 通过不必要的程序（PUP）传播恶意代码

在正常的PC应用程序安装过程中，会安装一些协作应用程序。不必要的程序和恶意代码通过安全脆弱的合作应用程序提供商进行分发。还通过以Active X形式安装不必要程序的过程中嵌入其中并分发恶意代码。当不必要的程序的更新文件被运行时，通过访问程序的更新服务器来检查是否存在更新文件。如果有更新文件，它会下载并执行它。此时，没有检查下载的文件是否被篡改。攻击者利用这个漏洞， 在特定时间将更新文件更改为恶意代码并进行分发。分发的恶意代码内部结构如下所示，是结合了生成不必要的程序（PUP）文件的行为代码和执行恶意行为的代码的形式。

■ 通过易受攻击的网站分发恶意代码（Drive By Download）

易受攻击的网站和以广告目的制作的网站长期以来一直是攻击者的猎物。攻击者不仅可以隐藏自己的位置持续攻击，而且根据广告页面曝光的频率将恶意代码传播和分发给不特定多数用户。多年来IT安全报告中已经出现了有关易受攻击的网站和广告主页的警告信息。然而，攻击者变得更加细致周到，至于可以在自己限定的时间传播恶意代码。切记：即使是用于广告目的的且没有任何变化的网站，在任何时刻都有可能变成恶意网站并传播恶意软件，还诱导用户访问该恶意网站后输入个人信息以导致泄露个人信息和导致金融损失。



【图 7】通过易受攻击的网站分发恶意代码

与生活密切相关的安全威胁之三，伪装成正常文件的恶意代码

为了欺骗用户，首先，攻击者将恶意代码伪装成一个普通的文件。与此相关的方法是根据PC环境和IT技术的发展而发生变化，但这并没有大大脱离了欺骗用户的方法的范畴。攻击者可以直接使用Windows的正常文件名，或伪装成可信应用程序的图标和应用程序名称。

在办公室环境中，伪装成文档文件后引诱用户点击的情况较多；有时还伪装成费用通知单等在线服务相关的内容。这些恶意代码基本上都收集用户的个人信息，并在用户访问的基础设施中收集私人和公共数据，还控制PC和服务器后，根据攻击者的意图进行各种活动。攻击者在达成攻击目的之后，有时会删除恶意代码后悄悄离去。但在有些情况下，PC可能会被破坏，从而无法再使用。

主要恶意软件诊断名	PDF/Phishing, Trojan/Win32.Delpiloader, Trojan/Win32.Bladabindi 等
类型	特洛伊木马（Trojan，收集和泄露用户信息为目的）
目标系统(OS)	Windows
主要行为	收集•泄漏用户信息，控制感染PC
其他特点	根据攻击者的意图，它可以用作僵尸PC来利用在其他攻击
预防方法	- 将V3更新到最新版本后，启用实时监控 - 文档文件或新的安装程序尽可能通过可靠地途径获取和使用
AhnLab解决方案	V3, MDS(恶意代码诊断•删除)

【表 3】 伪装成正常文件的恶意代码攻击的主要特点和响应方案

伪装成正常文件的攻击的主要事例

■ 伪装成正常实用程序的恶意代码

在过去，攻击者将恶意代码伪装成有名的程序，特别是流行的实用程序和视频文件。最近发现的后门恶意代码也被伪装成韩国有名的压缩程序。

此外，伪装成Adobe Flash更新程序的一个名为setup.exe的勒索软件（Ransomware）被分发。它没有文件图标，而且分发的文件名“Flash_update”，但版权说明却是“Firefox and Mozila”。 如果用户发现这几个特点，有可能可以避免被感染。然而，在典型的PC环境中，用户只因为文件名为“setup.exe”这一点，就丝毫没有怀疑地运行并被感染勒索软件。

■ 伪装成文档文件的恶意代码

恶意软件作者将恶意文件伪装成简历表，诱导人力资源部和招聘人员运行该文档文件。伪装成文档文件的该文件在运行时自动解压缩。当运行伪装成简历表文档文件的恶意代码时，由于正常的PDF文档格式的简历表文件也同恶意文件一起生成，用户难以判断恶意文件被云行。

创建在与文档文件相同文件夹的恶意文件具有隐藏的属性，因此到Windows浏览器菜单的 [工具] - [文件夹选项] - [查看]中，取消“隐藏受保护的操作系统文件（推荐）”选项，则可以看到隐藏属性的恶意文件。

恶意代码使用无效的假证书进行签名。虽然签名时间是最近，但如果仔细查看签名信息，可以看到它是无效的证书。恶意代码旨在不断与攻击者进行通信，以收集信息，渗透受感染的PC，并执行其他命令。

■ 伪装成视频文件的恶意代码

有一种叫做Torrent的在线服务，用户可以通过该程序搜索更多的隐秘的资料。Torrent是一种在个人之间相互传输文件的协议，也是使用该协议的应用程序的名称。

Torrent服务允许用户通过Internet分发、存储和共享文件，并通过多个连接从多个位置同时获取文件，因此您可以享受快速的传输速度。提供此类Torrent服务的公司可通过公开的公告栏发布可下载的文件，任何人都可以通过搜索轻松访问，并引导用户使用他们的服务。此外，网络社区公告板通常包含具有刺激性标题的Torrent文件，以吸引高下载量。

恶意文件使用视频播放器图标，文件扩展名使用了视频扩展名“*.mp4”伪装成视频，但该文件是恶意代码。当该恶意代码被运行，生成实际的视频文件并将其显示给用户，因此用户难以识别该文件是恶意代码。在用户观看视频的时候，攻击者则通过恶意代码来做准备收集用户信息和执行远程命令。

最后...

此时此刻，攻击者正在IT环境中寻找安全漏洞，并准备下一个网络攻击。他们通常希望通过网络攻击可以兑现。在黑市销售个人信息到窃取金融信息并转账，一切都与金钱有关。虽然各种安全系统正在保护个人和企业信息，但攻击者可绕过防御系统，为引发人为错误而持续攻击，双方的攻防之战仍在继续。

通过本文，希望读者牢记和注意“网络钓鱼”、“域欺骗”和“伪装型恶意代码”等在我们的日常生活中可能会遇到各种安全威胁。

AhnLab

安全月刊

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） | cn.sales@ahnlab.com