AhnLab

安全月刊

Vol. 30

最近的安全威胁

及对应策略

最近的安全威胁及对应策略

面对勒索软件•域欺骗•鱼叉式网络钓鱼的应对策略有哪些？

信息安全(Information Security)主要包括以下五方面的内容，即需保证信息的保密性、真实性、完整性、未授权拷贝和所寄生系统的安全性。[1] 在 IT 所说的信息安全是指在信息的收集、加工、保存、搜索、发送和接收过程中，为防止信息损坏、篡改和泄漏等的管理和技术方法。安全威胁(Security Threat)是指为了达到某种目的而实施的威胁信息安全性的行为。自信息安全的概念产生以来，出现了数多的安全威胁和多样的攻击方法，而这些安全威胁的中心就有恶意软件(Malware)。虽然并不是所有的安全威胁或高级攻击使用恶意软件，但是大部分的攻击都使用恶意软件，这是毫无疑问的。

本刊将介绍最近成为话题的利用恶意软件的安全威胁，如“勒索软件”、“域欺骗”和“鱼叉式网络钓鱼”等。另外，还介绍如何防范这些恶意软件，最后介绍利用 AhnLab MDS 产品的对应这些恶意软件的策略。

电脑或手机变“人质”，勒索软件

勒索软件(Ransomware)是黑客用来劫持用户资产或资源并以此为条件向用户勒索钱财的一种恶意软件。勒索软件通常会将用户系统上文档、邮件、数据库、源代码、图片、压缩文件等多种文件进行某种形式的加密操作，使之不可用，或者通过修改系统配置文件、干扰用户正常使用系统的方法使系统的可用性降低，然后通过弹出窗口、对话框或生成文本文件等的方式向用户发出勒索通知，要求用户向指定帐户汇款来获得解密文件的密码或者获得恢复系统正常运行的方法。[2]

勒索软件不是新的恶意软件，这种恶意软件在国外已经流行多年。最近，在亚洲也开始变得越来越普遍。去年，在韩国被报告PC被勒索软件感染事件发生之后，最近韩国的企业和机关陆续发生了被勒索软件感染事件。尤其，出现了针对移动设备的勒索软件和瞄准玩家比特币的勒索软件等，手法越来越精巧，受害事例也越来越增加。

勒索软件最常用的方法是，将病毒伪装成垃圾邮件的附件，发送到用户的邮箱之中。或者利用社会网络服务(Social Network Service)或门户网站(Portal Site)传播恶意软件。

【图 1】索要比特币的勒索软件

[1] 百度百科

[2] 百度百科

当用户点击邮件附件的病毒文件，勒索软件已经入侵到用户的计算机之中。在该勒索软件感染用户计算机之后，即会在桌面显示勒索信息，并将计算机上的私人文件和图片被加密导致无法打开。如果用户不支付赎金，文件将可能永久无法解密。赎金要求通过 Paypal 等在线支付或比特币等虚拟货币。

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。

【图 2】 将文件加密后索要赎金的“CryptoLocker”

当用户被勒索软件感染，即使支付了赎金，但是无法将所有的文件恢复正常。因此，重要的还是事前预防。下面了解一下有关勒索软件的防范和被勒索软件感染以后恢复加密数据的方法。

最近被报告的勒索软件大部分是通过垃圾邮件扩散。一旦被感染，用蛮力破解加密文件几乎是不可能的，而且不支付赎金将会失去一切。

为了预防被勒索软件感染，需要做到下面几点：

- ✓ 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；
- ✓ 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的网盘；
- ✓ 积极更新你的防病毒软件和操作系统。

将重要文件设置为“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。

针对用户电脑的桌面勒索行为的案例持续增加，并延伸至智能手机，而大部分病毒针对安卓系统。移动勒索软件入侵智能手机，将智能手机中的个人信息作为“人质”要求赎金。与桌面勒索软件相比，移动勒索软件被认为更容易防御。

为了预防移动勒索软件，需要做到如下几点：

✓ 不要下载 Google Paly 或 App Store 等官方商店之外的应用，最好设置“来源不详”为禁用；
✓ 官方商店也有可能下载到恶意应用，需要确认使用评判后下载；
✓ 避免点击短信或SNS上的链接；
✓ 安装一款可封杀勒索软件的应用。

如果您的手机被感染勒索软件，将手机以安全模式重新启动，然后到【设置 -> 手机管理】菜单，将包含勒索软件的应用设置为禁用。再到应用列表删除该应用即可。

假的逼真，域欺骗(Pharming)

域欺骗(Pharming)是借由入侵DNS或代理服务器，将使用者诱导到伪造的网站并盗取个人信息的一种攻击方式。最近域欺骗攻击很多利用在盗取使用者的金融信息。即，先感染使用者的电脑后，当使用者访问网上银行时，将使用者引导到伪造的银行网站，并盗取个人金融信息。

目前攻击者为传播域欺骗恶意软件而最多使用的方式如下：

■ **恶意软件隐藏在其他程序后传播**：将窃取网上银行信息的恶意软件隐藏在网络硬盘程序或可能不需要的程序(Potentially Unwanted Program, 简称为PUP)内。即正常运行这些程序后，恶意软件在后台运行。当用户访问银行网站时，不知不觉中却持到仿冒的网站上，盗取用户的证书并诱导用户输入安全卡号码等重要信息。这种情况下，因为下载的程序内隐藏着恶意软件，用户全然不知自己访问的银行网站是假的网站，便毫不犹豫地输入要求的金融信息。
■ **通过伪造漏洞网站的传播**：选择一个访问人数多且网页存在漏洞的网站，然后伪造部分网页来传播攻击者制作的恶意软件。此时，利用JAVA漏洞的情况较多。因为是经常访问的网站，用户根本就不怀疑该网站是假的。

为了防止域欺骗，需要做到如下几点：

✓ 首先将安全更新和使用杀毒软件等基本的安全守则做到日常化；
✓ 禁止下载来源不明的文件；
✓ 禁止点击来源不明的电子邮件附件；
✓ 证书最好保存到U盘等移动式存储设备，不要保存在电脑；
✓ 网上进行金融交易时，除了证书和安全卡之外，最好使用额外的验证方式。

特别注意，没有一家金融机关要求你输入所有的金融信息。因此，过分要求输入金融信息的时候，要起疑心并拒绝输入信息。另外，如果你的电脑已被域欺骗恶意软件感染，请迅速将证书作废并重新申请安全卡。

利用用户心里的针对性攻击，鱼叉式网络钓鱼

鱼叉式网络钓鱼(Spear phishing)是一种源于亚洲与东欧只针对特定目标进行攻击的网络钓鱼攻击。由于鱼叉式网络钓鱼锁定之对象并非一般个人，而是特定公司、组织之成员，故受窃之资讯已非一般网络钓鱼所窃取之个人资料，而是其他高度敏感性资料，如智慧财产权及商业机密。[3]

当攻击者锁定目标后，通过电子邮件，假冒该公司或组织的名义发送伪装成附件的病毒，诱使用户点击该附件。该攻击方法是很传统且最普遍的攻击方式，但是这种方式的成功率仍然很高。因此，安全专家们指出“安全最大的漏洞是人”。

您可以根据下面的特性来区别垃圾邮件和鱼叉式网络钓鱼邮件。

▲锁定对象并非一般人，而是特定公司、组织成员(针对性)
▲并非一般的窃取个人信息，而是其他高度敏感信息，如公司机密、系统破坏等(严重性)
▲看起来跟一般的正常文件没有区别(精巧)

鱼叉式钓鱼经常被利用在高级持续性攻击等网络攻击。如要从鱼叉式钓鱼攻击保护个人和所属组织，需要提高个人的安全意识，还需要所有人共同努力。

[3] 百度百科

企业和机关要充分认识到鱼叉式钓鱼攻击的严重性，并从全方位的观点建立响应方案，尤其要掌握 APT 等高级网络攻击如何利用鱼叉式钓鱼。通过鱼叉式钓鱼攻击入侵到企业内部的恶意软件大部分是针对特定对象而定制。因此，需要考虑防御已知恶意软件的防病毒软件，还需要考虑防御未知恶意软件的多层次的安全解决方案。另外，定期进行安全教育和培养内部安全负责人等也要做好。

做好上述的技术措施的基础上，再加上个人的关心和努力的话，对于防御鱼叉式钓鱼攻击可能很有效果。

- ✓ 首先，只要感觉到一点点的可疑的地方，请不要随意打开邮件附件或链接。这是阻止鱼叉式钓鱼攻击的最为有效的方法。
- ✓ 然后，对于经常使用的应用软件，即时应用该应用软件公司提供的安全补丁和更新。因为，利用文档等 Non-PE 型文件的鱼叉式钓鱼攻击呈现增加趋势，更新软件相当重要。
- ✓ 最后，即使已打开可疑邮件附件或点击链接，请不要慌张，赶紧联系公司的安全负责人，使采取有效措施。

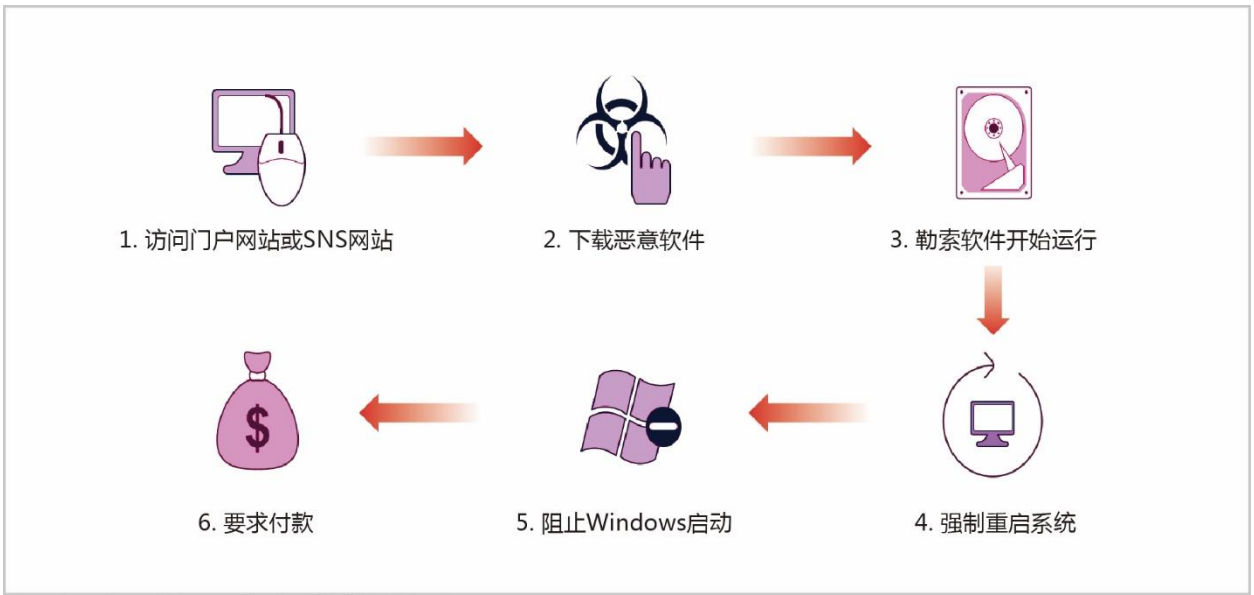
AhnLab Malware Defense System (MDS)

AhnLab MDS 是检测高级持续威胁 APT(Advanced Persistent Threat)等日益进化的最新安全威胁，并通过专用 Agent 实时响应的下一代安全解决方案。下面将详细介绍 AhnLab MDS 如何响应“勒索软件”、“域欺骗”和“鱼叉式网络钓鱼”等高级安全威胁。

1. 勒索软件攻击及其对应流程

攻击者首先将伪装成最近流行的“屏保程序”，并将安装程序登记到用户经常访问的门户网站博客或 SNS 网站。用户丝毫没有怀疑该程序，便下载到电脑后安装。但是，该程序运行的同时病毒文件也随之下载并安装到用户的电脑中，用户的电脑即被勒索软件感染。

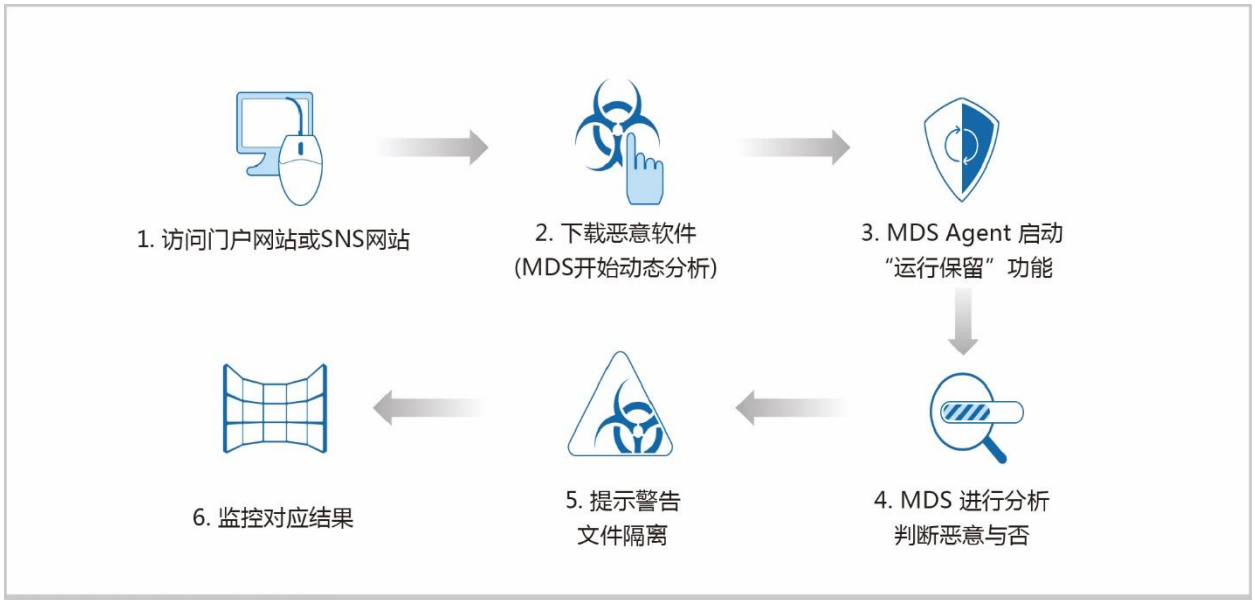
当用户欲打开电脑里的文件或照片时，发现文件和照片被莫名其妙的加密了。有些勒索软件有可能将整个硬盘加密。随后屏幕上会弹出一条勒索软件特有的要求赎金的勒索消息。攻击者给出一个期限，如果该期限之内没有支付赎金，用户的文件和照片，或者整个硬盘永久被加密，甚至还有可能被攻击者彻底损毁。



【图 3】通过门户网站或SNS下载程序后被勒索软件攻击的流程

那么，在相同被勒索软件感染的情况下，AhnLab MDS 如何有效对应呢？

如【图 4】所示，当用户通过门户网站或 SNS 网站下载伪装成正常程序的恶意软件时 MDS 便开始动态分析。在勒索软件运行之前，MDS Agent 判断该文件判断为“具有可疑行为的新的可执行文件”。首先，对该文件进行“运行保留(execution holding)”措施。然后，MDS Agent 将该文件传送到 MDS 进行分析。MDS 分析结束后将其结果传送到 MDS Agent。如果是恶意文件，则对该文件进行删除或隔离措施，最终可以从勒索软件中安全保护用户的电脑。



【图 4】AhnLab MDS 对应勒索软件的过程

2. 域欺骗攻击及其对应流程

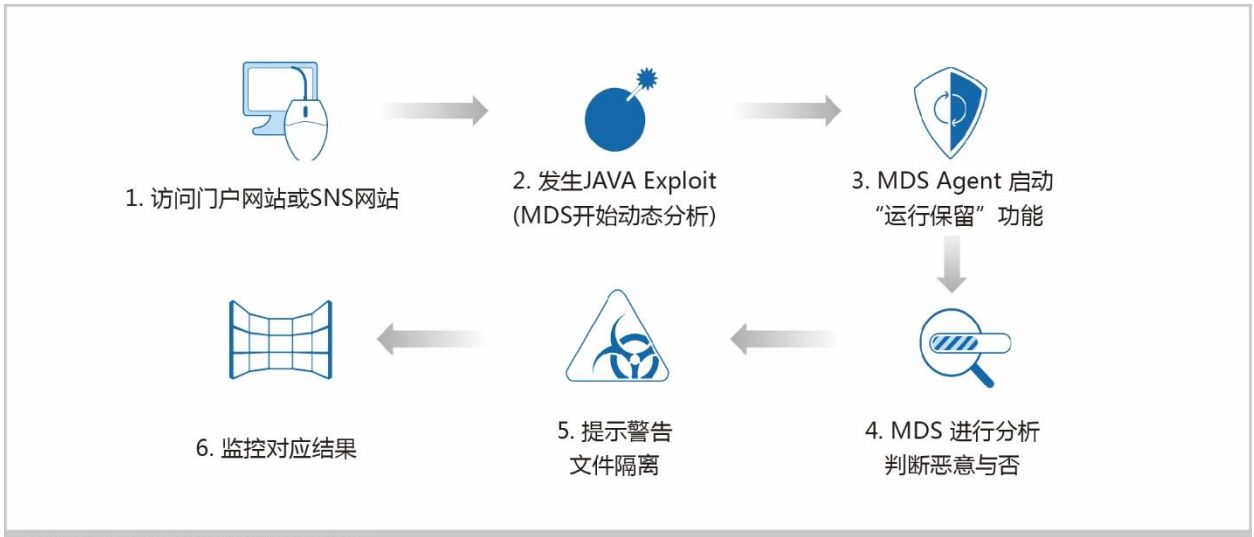
域欺骗攻击与勒索软件攻击不同，勒索软件攻击是通过用户自发点击而开始，但是域欺骗攻击是在用户不知不觉的状态下自动安装恶意软件。攻击者首先准备一个包含 Exploit 的网站，然后利用 Java 漏洞在用户不知情的状态下感染用户电脑。该网站通常使用预先已攻击的 Web 服务器。漏洞攻击对象是用户电脑中安装的 JVM(Java Virtual Machine)软件，运行任意的命令。当用户访问特定网站的时候，通过“水坑式攻击(Watering-hole)”在用户不知不觉的情况下感染域欺骗恶意软件。

该恶意软件将自己登记到 Windows 启动项目和服务中，计算机启动时便自动运行，并篡改 hosts 文件。当用户访问特定银行网站时，引导访问攻击者早已准备的虚假的地址，看起来与该银行的官方网站非常相似，但实际上是欺诈网站。这些欺诈网站往往提示用户输入其账户信息， 如信用卡号、帐号、口令等信息，很多用户毫不怀疑地输入个人敏感金融数据。骗取用户个人敏感信息后，攻击者利用这些信息登录到实际银行官方网站，将用户的存款盗走。

【图 5】银行网站的域欺骗攻击流程

那么，在相同被域欺骗恶意软件感染的情况下，AhnLab MDS 如何有效对应呢？

当攻击者通过 Java 漏洞攻击，将恶意文件下载到用户计算机并欲运行时， MDS Agent 判断该文件为“具有可疑行为的新的可执行文件”，首先对该文件进行“运行保留(execution holding)”措施。MDS Agent 将该文件传送到 MDS 进行分析。MDS 分析结束后将其结果传送到 MDS Agent。如果是恶意文件，则对该文件进行删除或隔离措施，最终从域欺骗恶意软件中安全保护用户的电脑。



【图 6】AhnLab MDS 对应域欺骗恶意软件过程

3. 鱼叉式网络钓鱼及其对应流程

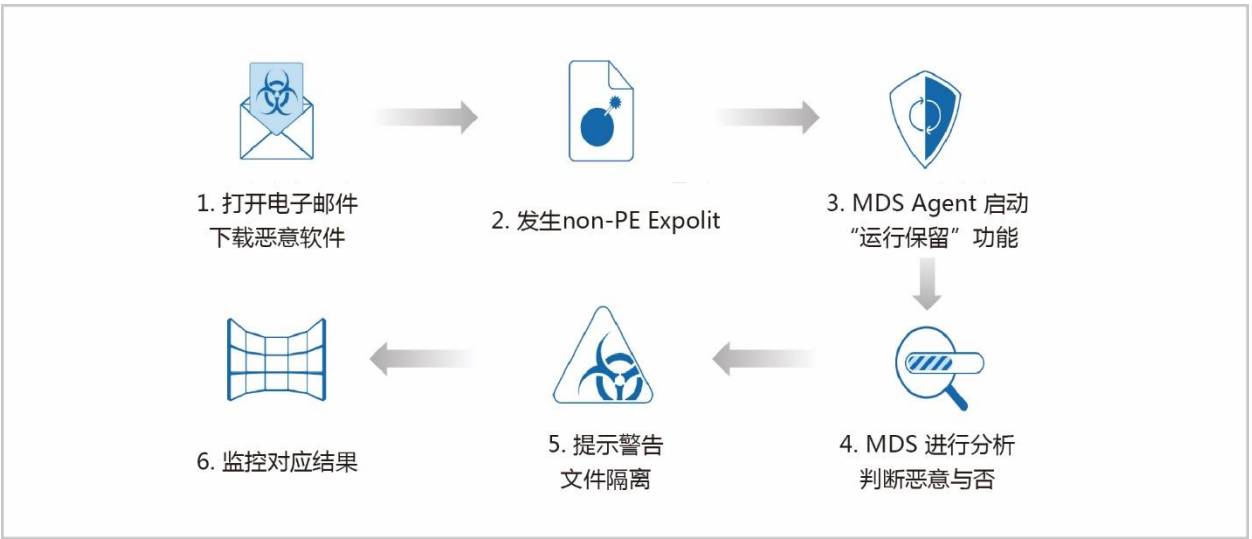
在鱼叉式网络钓鱼攻击中，攻击者针对特定公司或组织成员，制作与他们的业务领域相关的一些文档并通过电子邮件发送到锁定的目标的电子邮箱中。攻击者还很周密地将恶意软件进行加密妨碍其他网络安全设备的分析，并通过 SSL 流量下载“键盘记录恶意软件”。

用户一旦点击打开文件都会感染病毒，计算机被安装键盘记录病毒。通过该病毒，公司内部重要的数据将传送到外部的 C&C 服务器。之后，攻击者将安装“远程控制程序”，通过该计算机访问公司内部的计算机，并窃取重要的信息。

【图 7】鱼叉式网络钓鱼攻击流程

对于上述的通过电子邮件的鱼叉式网络钓鱼攻击，AhnLab MDS 以独特的技术对应。

当电子邮件附件设置了密码，如果在邮件本文中可以提取到解密用密码，则可以通过动态内容分析技术(Dynamic Intelligent Content Analysis, DICA)，不管该文件的可疑与否，能够准确地检测到应用程序的零日漏洞。



【图 8】AhnLab MDS 对应鱼叉式网络钓鱼攻击的过程

如果，即使中间没能提取到密码，并且在网络也没能检测到通过 SSL 流量下载到的“键盘记录恶意软件”，MDS Agent 通过“运行保留(execution holding)”功能阻止可疑文件在用户的计算机中运行。

到目前为止，我们了解了 AhnLab MDS 如何应对“勒索软件”、“域欺骗”和“鱼叉式网络钓鱼”等的攻击。在应对这些攻击过程中收集到的新的恶意软件的信息将通过 AhnLab 云分析系统反应到 AhnLab 防病毒产品 V3、移动安全产品 V3 Mobile、网络安全产品 TrusGuard 等 AhnLab 所有的安全产品的特征码和规则数据库。

最后，我们可以总结出，如要应对和防御“勒索软件”、“域欺骗”和“鱼叉式网络钓鱼”等恶意软件，需要人、技术和流程的相互协调。即“优化于公司 IT 环境的安全技术”、“执行安全业务的流程”和“组织成员对安全认识的改善”尤其重要。

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