Keywords A to Z Vol.12

Keyword 恶意软件[Malware]

恶意软件是指通过电子邮件等途径入侵计算机，进行机密信息窃取或数据的破坏和篡改等“恶意行为”的软件总称。

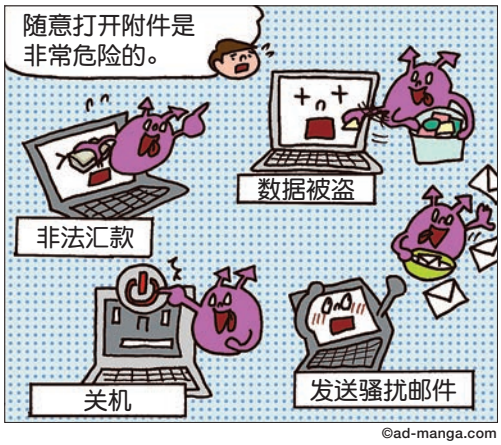
对计算机的使用造成威胁的“恶意软件”的恶意行为

如今，在企业的商业活动以及我们的日常生活中，IT 和网络已经成为不可或缺的一部分。而另一方面，“恶意软件”的威胁日趋严重。恶意软件（Malware）这个词源自“Malicious（有恶意的）”和“Software（软件）”。恶意软件可侵入计算机，窃取计算机中保存的个人数据等机密信息，或破坏和篡改数据，顾名思义，就是开展“恶意”行为的软件。

这种恶意软件一般通过电子邮件或外部存储媒体来感染非特定用户的计算机，在攻击的同时，通过网络等途径感染其他计算机。因此，“计算机病毒”这一名称被大家所熟知。例如，2000 年在全球范围内爆发的“LOVELETTER”计算机病毒，通过随机发送标题为“I Love You”的电子邮件，诱导用户打开附件，并不断向接收者计算机通讯簿中的邮箱地址发送自己的副本，进行扩散。当时的“I Love You”病毒基本上不会对数据进行窃取、破坏或篡改等，只是让病毒在全世界的用户中蔓延，属于“以犯罪取乐”。

但是，近年来出现了以扰乱或威胁组织为目的、进行“针对性攻击”的恶意软件。近年来出现的病毒经常开展远远超出现有病毒框架的各种行为，有明确的犯罪意图，企图从企业、国家或地方政府的组织系统中窃取机密信息或篡改数据。这些软件统称为恶意软件。

不仅是组织机构，恶意软件对我们个人也已造成严重的威胁。最近快速传播的“勒索软件”就是其中之一。它与其他恶意软件一样，通过邮件附件等途径感染，对计算机上的数据进行加密。用户无法访问需要的数据时，攻击者会发出邮件，要求付款来解除密码。也就是以计算机中的数据为“人质”来要求“赎金”。



©ad-manga.com

如何应对与便捷如影随形的恶意软件威胁

对于日趋恶劣的恶意软件，需要采取更强有力的对策。企业等大多数组织机构都会在计算机或服务器上安装杀毒软件，作为一般的防恶意软件对策，如在公司的网络入口或内部建立起防火墙等，同时完善多重防御体系。此外，还会推进使用上的强化对策，如要求员工严格遵守“绝不打开邮件中的可疑附件”等规章。

但是，针对性攻击的受害者还是源源不断。杀毒软件的工作原理是与已有恶意软件的结构进行比对，将匹配的软件视为威胁入侵进行检测，因此很难检测到用于攻击特定组织的被自定义的恶意软件。此外，有些恶意软件还会钻使用规章的空子，比如伪装成上司、同事、熟人的邮件，诱骗用户打开附件。

所以，很难完全防止恶意软件的入侵。因此，除了采取传统的对策外，“入侵后”对策的重要性也日益提高，比如，如何在侵入后掌握恶意软件的活动等。

而对于个人而言，又能采取哪些措施呢？与组织机构一样，必须在计算机或智能手机上安装杀毒软件，并及时更新浏览器或软件，同时，绝对不可打开可疑附件。此外，在访问不常用的网站时，还应该特别注意网站的可靠性。网站的访问与邮件一样，是恶意软件的主要侵入途径。

IT 和网络的使用为我们的社会带来了巨大的便捷。然而，便捷和恶意软件的威胁如影随形。我们应时刻意识到自己暴露于风险之中，积极获取恶意软件的相关信息，将机密数据转移到磁盘等中，而不是放在计算机上，除了邮件之外，还需要电话、传真等多种通信方式组合使用。用户需要切实采取平时能够做到的对策，确保安全使用。

封面照片由水谷孝次提供，选自MERRY PROJECT

azbil

http://www.azbil.com/cn/

2012年4月1日，株式会社 山武 已更名为 阿自倍尔株式会社。

azbil集团宣传杂志 azbil（阿自倍尔） azbil 2017 Vol.2，No.7

发行负责人：阿自倍尔株式会社 经营企画部广报组 高桥实加子

日本国东京都千代田区丸之内2-7-3 东京大厦19层 TEL：81-3-6810-1006 FAX：81-3-5220-7274

PRINTED WITH SOY INK

MIX Paper from responsible sources FSC® C002215

PR-3001C-1704（1704-2K-D）

Company/Branch office