AhnLab

安全月刊

2017.06 Vol. 55

V3 诞生 29 周年

V3诞生29周年，其功能越来越强大

完全攻略2017年版V3强大的安全功能

1988年6月1日，韩国第一个防病毒（Anti-Virus, AV）程序V3诞生。为治疗被称为最初的计算机病毒的“脑”病毒而开发的V3在29年的时间迎合IT环境的变化而不断发展。其结果，它不仅提供了各种功能使可以安全、方便地使用计算机，还可以迅速响应包括最近急增的勒索软件的大量新种和变种恶意软件。

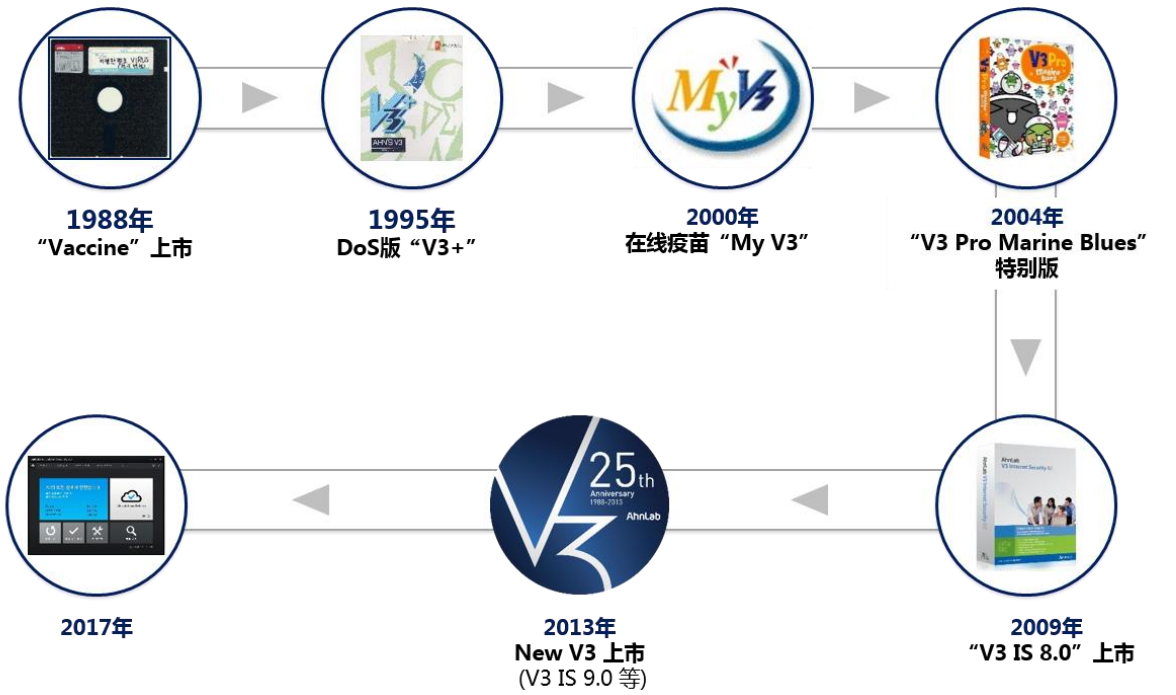
V3是病毒的英文拼写“Virus”的第一个字母“V”和1991年发布最多的第三版本的数字“3”的组合。之后，V3凭借广泛知名度，在韩国成为了一个品牌。目前，V3的个人版产品有“V3 365”、“V3 Lite”、“V3 Internet Security 9.0(以下称为V3 IS)”；企业版产品有“V3 Endpoint Security 9.0”、“V3 Net for Windows Server 9.0”、“V3 Net for Unix/Linus Server”；移动版产品有“V3 Mobile Security”和“V3 Mobile Plus”等，这些V3产品群作为AhnLab主要产品的母品牌而位于其中心。

回顾今年迎来29周年的V3，本刊将介绍2017年版V3强大安全功能，并阐述如何充分利用V3来保护计算机安全。

29年的演变：V3显示了IT历史

随着脑病毒（1988）、耶路撒冷病毒（也称为“星期五病毒”，1989年）、米开朗基罗病毒（1991年）相继出现，“疫苗”也迅速发展为 VⅡ Plus（V2 PLUS）和 V Ⅲ（V3）。特别是在1991年4月，米开朗基罗病毒的传播成为了V3开始被大众获得认可的契机。

最初的V3只是为了治疗当时出现的恶意代码而制作的。然而，随着IT技术的进步，恶意代码种类也开始增加，AhnLab迎合IT环境的变化，持续发展技术，以抢先应对新的威胁。随着IT环境变化而发展的V3的核心技术如下：Dos版计算机防病毒软件“V3 +”、在线防病毒软件“My V3”，韩国第一款移动防病毒软件“V3 Mobile for Palm”，2000年代推出了应用了基于云计算的ASD技术（V3 IS 8.0），接着在2013年推出了应用基于信誉和行为等分析技术的平台的新的V3（V3 IS 9.0等）。接着在2016年，为了应对勒索软件，应用了诱饵（Decoy）技术，并添加了安全文件夹功能。



【图 1】 V3的主要变化

2017年版V3，有什么新的变化？

通过V3的发展，可以看到当时最严重的安全威胁是什么。要说到2017年最严重的安全威胁，无疑是勒索软件（Ransomware）。2017年版 V3，它可以保障用户PC环境安全，以及诊断和处理传统的恶意代码，如“间谍软件”和“木马程序”，以及当前最恶劣的恶意软件“勒索软件”。下面让我们仔细了解以下2017年版V3的各种功能。

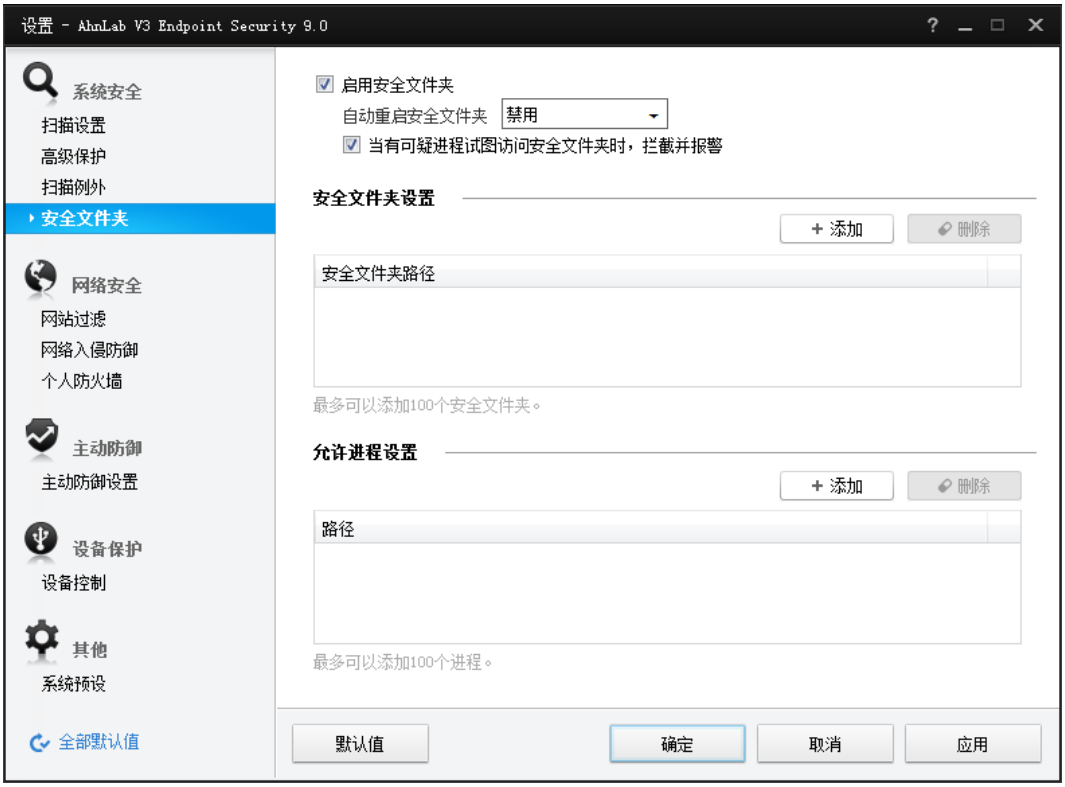
应对勒索软件

最近，Wanner Cryptor（又称Wanner Cry）勒索软件在全球150个国家感染了超过30万台电脑，这个勒索软件利用了Windows操作系统的SMB（Sever Message Block）漏洞。

相对其他国家，韩国被Wanner Crypto勒索软件受到的损害并不大，但持续出现了Wanner Cryptor的变种。另外，令人担忧的是利用SMB漏洞的各种类似攻击。5月底，AhnLab在其V3产品上应用了IPS（Intrusion Prevention System, 入侵防御系统）特征码检测技术，以阻止SMB漏洞攻击流量。由此，V3不仅可以检测和删除当前的Wanner Cryptor勒索软件，还可以应对包括Wanner Crytor变种的利用该漏洞的其他攻击。

在此之前，2016年6月，AhnLab应用了“诱饵（Decoy）诊断”技术，以加强V3产品对新种和变种勒索软件的诊断。诱饵诊断是一种使用诱饵来引诱勒索软件的技术，它可以检测并阻止试图利用特定文件和文件夹来加密或更改文件名的程序。它在根（Root）路径中创建一个诱饵文件夹，即使启用了“隐藏文件夹选项”，用户也看不到诱饵文件夹和文件，从而最大限度地减少了用户的不便。 此外，还添加了通过多个文档篡改检测勒索软件的功能。一些勒索软件在感染系统后以随机顺序加密文件和文件夹，V3则可以检测更改多个文档的行为，有效地应对了这种类型的勒索软件。

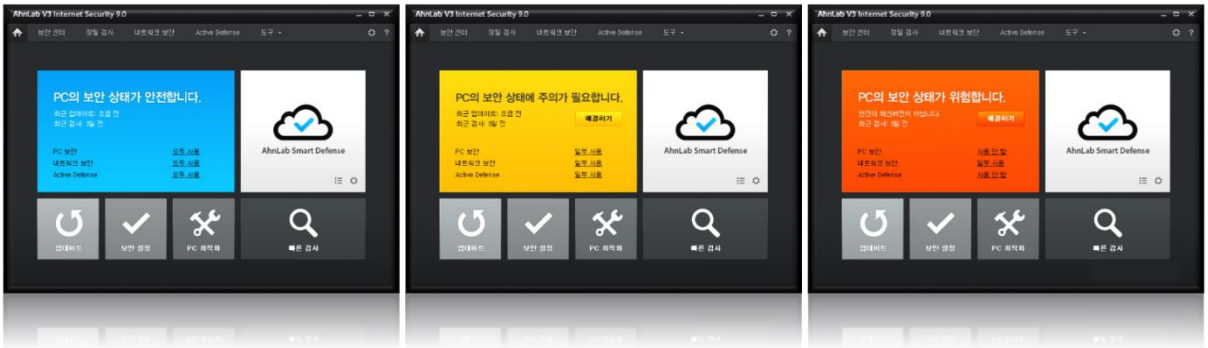
V3特别受到注目的是为了应对勒索软件而新增的“安全文件夹”功能。安全文件夹功能可以阻止文件夹中文件的修改或删除以及新文件的创建，即使勒索软件已入侵到计算机中，无法加密被指定为“安全文件夹”的文件夹中的文件。勒索软件的预防措施之一是数据备份，这需要一定的时间，也可能会有点麻烦，而V3的安全文件夹功能可以通过简单的设置来防止重要文件被加密。AhnLab通过收集用户的意见，不断提高安全文件夹功能的可用性。



【图 2】 V3的“安全文件夹”设置界面

“基本功”扎实的V3

V3提供直观的用户界面，如【图 3】所示，使用户可以一目了然地掌握计算机的安全状况。V3使用不同的颜色来显示计算机安全状态。“蓝色”表示安全状态；“黄色”表示注意状态；“橘黄色”表示危险状态。
但是有些用户说道，当计算机处于“危险”或“注意”状态时，不知采取何种措施。此时，用户可以利用“解决”按键，它会自动检测计算机后将计算机防护设置为安全。另外，还可以使用“快速扫描”功能，快速扫描和诊断计算机。



【图 3】根据计算机安全状态显示不同颜色的V3主界面

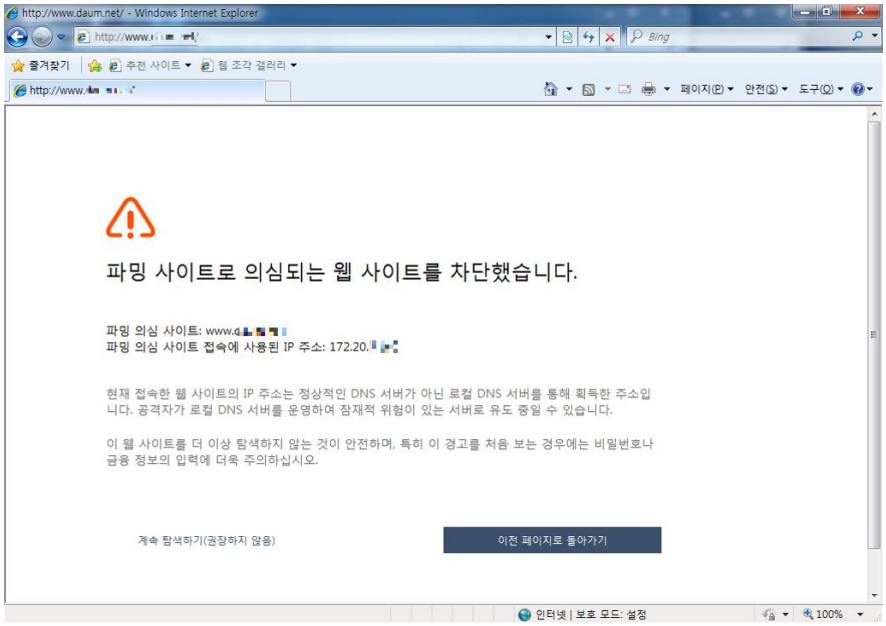
当计算机状态处于“危险”或“注意”时，V3的主界面出现“解决”按键。当用户点击“解决”按键，V3会自动检查当前的引擎版本、实时系统扫描启用与否等设置，并将设置自动更改，使计算机维持安全的状态。

您还可以点击V3主界面的“快速扫描”，快速且准确诊断和修复恶意代码。V3的基本功能包含了通过基于行为和信誉诊断来响应潜在的安全威胁。全盘扫描对系统的所有领域进行扫描，而快速扫描与此不同，它仅选择重要文件夹，如内存/进程、引导扇区进行扫描，从而缩短了扫描时间，减轻了用户的负担。快速扫描可以直接在V3主界面或任务栏的托盘图标运行。

可以预防域欺骗网站

当前不断增加的安全威胁之一有“域欺骗（Pharming）”。域欺骗是诱导用户访问假冒的金融网站后，窃取用户的个人信息和金融信息的一种攻击手法，需要用户的格外注意。然而，由于假冒的网站被攻击者制作得与实际网站很相似，用户很难区分开来，从而使用户不知不觉中被攫取个人信息。

为了保护用户免受这种高级的域欺骗攻击，V3提供“检测域欺骗行为”功能，当用户访问域欺骗网站时，阻止该连接，并显示如【图 3】的拦截界面。如要使用该功能，需要启用基于行为的入侵防御功能。



【图 4】V3检测域欺骗行为后弹出的拦截界面

更多V3的附加功能

V3除了提供防病毒软件之固有的功能之外，还提供了有用于个人计算机和互联网生活的各种功能。其中，最广泛使用的一个功能就是“系统优化”。计算机运行速度缓慢的原因除了被恶意软件感染，还有很多原因。当开机速度或互联网连接速度缓慢，又或者程序运行不正常，您可以使用V3的“系统优化”功能空出更多的系统资源，有效支配，并提高计算机的运行速度。
如果你是一个企业安全管理员，你还可以利用V3的“计算机扫描活动（PC Scan Campaign）”。如果启用该功能，当计算机在一段时间没有进行扫描，V3则弹出提示窗口，让您进行全盘扫描。此外，还可以通过“预设扫描”功能，使系统在指定的扫描时间自动进行扫描，保持计算机的安全状态。

AhnLab将通过6月末推出的定期补丁升级V3产品的恶意软件诊断和修复功能。最近在全世界流行的WannaCryptor勒索软件事件告诉我们：只要遵守最基本的安全守则，恶意软件带来的损害可以降到最低。如果您使用V3提供的各种功能，会是锦上添花。

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