AhnLab

安全月刊

2022.10 Vol.119

Lazarus Rootkit 攻击分析报告

Lazarus Rootkit 攻击使企业安全系统失效

最近，发现了由朝鲜黑客组织Lazarus传播的Rootkit恶意软件。该恶意代码会恶意利用易受攻击的驱动内核模块，使整个企业的安全系统陷入瘫痪。考虑到该攻击的设计复杂程度和Lazarus组织的攻击频率，需要各企业予以格外的注意。

AhnLab一直在密切关注Lazarus组织的攻击动向，并基于此公布了一份报告，详细介绍了该Rootkit恶意代码的攻击流程。在本文中，我们将简要介绍该报告的主要内容。完整的报告内容可以前往本公司的ASEC博客进行下载。

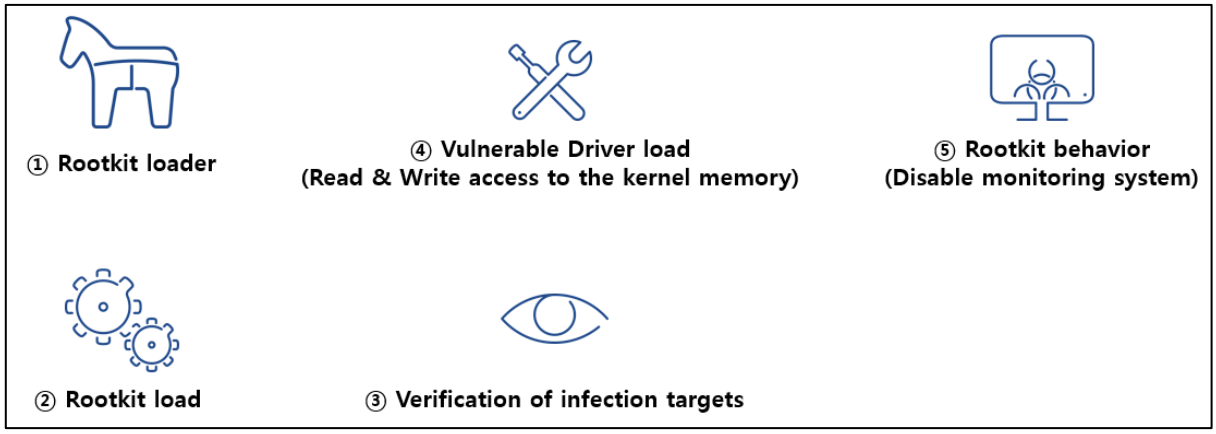
自2009年以来，Lazarus一直在对韩国、美国以及亚洲和欧洲的多个国家执行攻击。据本公司的ASD（AhnLab Smart Defense）基础设施发布的消息，Lazarus组织在2022年上半年对韩国国防、金融、媒体和制药行业发起了APT（Advanced Persistent Threat）攻击。

AhnLab一直在密切关注着Lazarus组织的攻击活动，并在此过程中确认了使安全产品失效的攻击情况。根据AhnLab的分析，Lazarus组织恶意利用过时版本的INITECH进程对企业进行初始入侵，然后从攻击者的服务器下载并运行Rootkit恶意代码。这里的Rootkit，是黑客用来防止系统用户识别他们被黑客入侵的工具。

产品失效攻击中确认的Rootkit恶意代码通过利用易受攻击的驱动内核模块直接对内核内存区域执行读取/写入操作。结果，导致系统中的所有监控系统均失效，包括防病毒软件（AV）。

Rootkit 恶意代码的运行方式

Lazarus组织使用的Rootkit恶意代码的运行过程（①~⑤）如【图1】所示。



【图1】Rootkit运行过程（①~⑤）

简言之，Rootkit以DLL形式在Rootkit加载器进程内存中运行。然后，在运行时，会在系统驱动路径中创建“易受攻击”的驱动程序模块（ene.sys），然后加载该驱动程序以修改内核内存区域的特定地址值。

由易受攻击的内核驱动篡改的地址区域是以DLL运行的Rootkit线程对象的PreviousMode地址，其值被修改为0。当用户线程对象的PreviousMode值变为0时，用户区域可以通过“NtWriteVirtualMemory”API访问内核区。

其后，攻击者会通过操纵用户区域中的内核内存使安全系统失效。该攻击的影响如此之大，以至于破坏了整个企业的安全系统，包括防病毒软件（AV），▲迷你文件过滤器、▲进程/线程/模块检测、▲注册表回调、▲对象回调、▲WFP网络过滤器、▲事件追踪等。此外，目标操作系统的范围很广，从Windows 7到Windows Server 2022。

Rootkit 攻击是如何发生的?

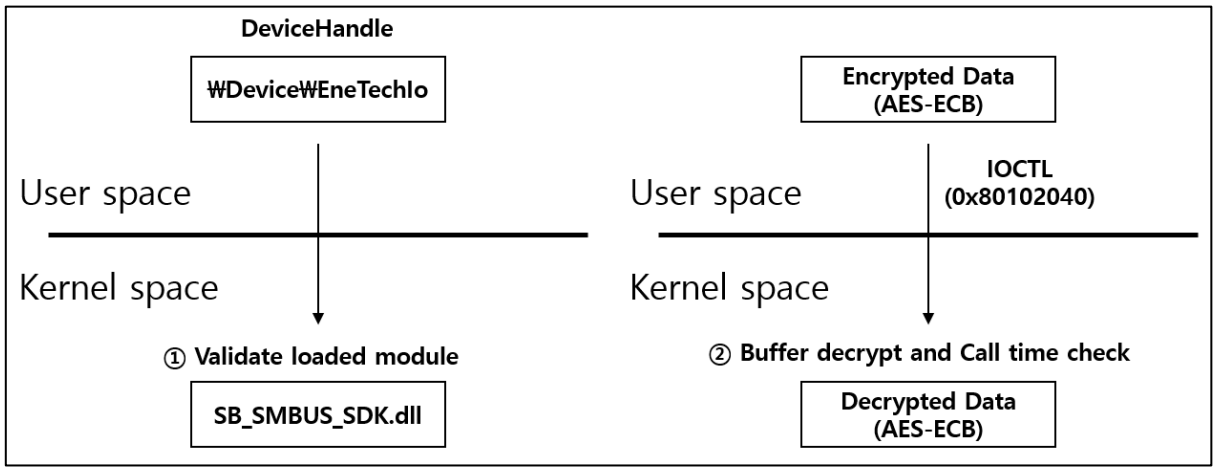
该攻击的核心在于“易受攻击的”驱动程序模块。

有一种称为为“BYOVD（Bring Your Own Vulnerable Driver）”的攻击技术主要使用来自硬件供应商的易受攻击的驱动程序模块进行攻击。尽管无法在最新的Windows操作系统中加载未签名的驱动程序，但攻击者可以利用易受攻击且带有合法签名的驱动程序轻松操纵内核区域。

在本次案例中，Lazarus组织使用的易受攻击的驱动程序模块是前面所提到的“ene.sys”模块。ENE Technology制作的ene.sys模块原样使用了Yariv Kaplan于1999年开发的“WinIO”开源库。

ene.sys模块有两个主要的安全问题，第一是在用户区域中映射物理内存区域的可能性。该模块实现了从用户区域直接访问内核的物理内存和I/O（Input/Output）端口，与ene.sys通信的用户进程可以通过IOCTL通信映射内核区域的物理内存。这意味着可以在用户区域对任意的内核物理内存区域进行操作。

第二是对调用者和数据的验证过程被设计为容易迂回。如【图2】所示，ene.sys验证SB_SMBUS_SDK.dll模块的加载（①），检查加载的模块是否为SB_SMBUS_SDK.dll，如果匹配，则将该进程识别为可信进程。在这里，加载SB_SMBUS_SDK.dll的进程可以实现与ene.sys驱动程序和IOCTL（Input/Output Control）的进行通信。



【图2】ene.sys调用者和有效数据的验证过程

【图2】的②表示有效数据验证过程。ene.sys计算调用IOCTL的时间与驱动程序接收和处理该IOCTL的时间之间的差值，以验证用户区域请求的IOCTL的有效值。此时，如果时间差小于2ms，则认为有效，并处理请求的IOCTL。

在这一验证过程中，通过简单的旁路操作，便可以读取/写入内核的任意内存区域。攻击者还以绕过验证的方式修改文件、进程、线程、注册表和事件过滤器等内核相关的全局数据，从而使系统中的所有监控程序失效。

AhnLab通过ASD基础设施分析驱动程序的分发路径，确认主要是通过笔记本制造厂商MSI的RGB内存模块控制模块进行分发。

攻击意义与预防策略

自Windows Vista应用了DSE（Driver Signature Enforcement）策略后，Rootkit的攻击似乎减少了。但，本文介绍的BYOVD（Bring Your Own Vulnerable Driver）攻击案例自2014年以来不断出现。到目前为止，被认为BYOVD攻击主要是为了提升权限。然而，Lazarus组织似乎是第一个发起精心设计Rootkit攻击使所有系统（包括从Windows 7到最新的操作系统Windows Server 2022）失效的组织，就像此次攻击。

AhnLab产品对此类恶意代码中的部分代码进行了诊断，并由ASEC跟踪该组织的活动来应对此类恶意代码。但是，不排除存在尚未发现因而没诊断出来的变种。

为了响应BYOVD攻击，微软在Windows 10的虚拟机监视器代码完整性（HVCI）模式和S模式中，根据阻止规则拦截不允许的驱动程序。像这样严格阻止驱动程序加载的措施目前被认为是防止此类攻击的最佳方法。

因此，企业安全负责人必须严格控制，禁止在一般用户环境中不加载驱动程序。此外，应更新安全软件至最新版本，已防止利用BYOVD进行APT攻击。

有关Lazarus组织的Rootkit恶意代码的详细分析，请查看完整的报告内容。

▶前往报告

AhnLab

安全月刊

https:// cn.ahnlab.com

https://global.ahnlab.com

https://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