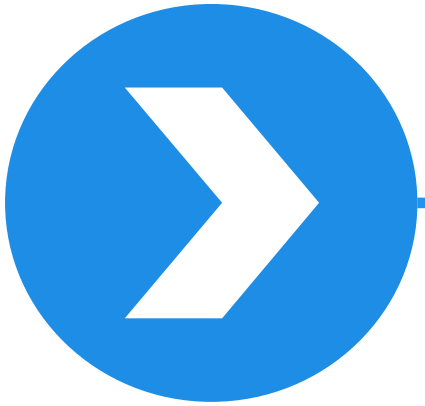
反Rootkit工具的发展演进

安天研究院

提纲

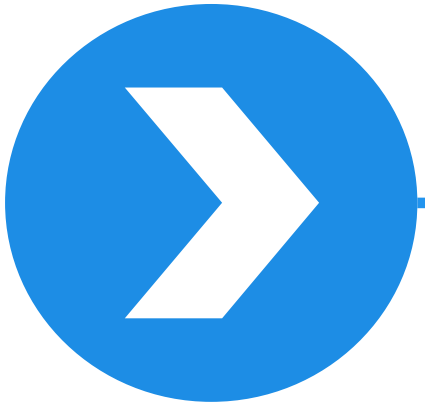
- 认识ARK工具
- 认识Rootkit
- Rootkit起源及威胁
- Rootkit的原理
- Anti-Rootkit的方法
- Anti-Rootkit工具
- 结束语



认识ARK工具

- Anti-Rootkit

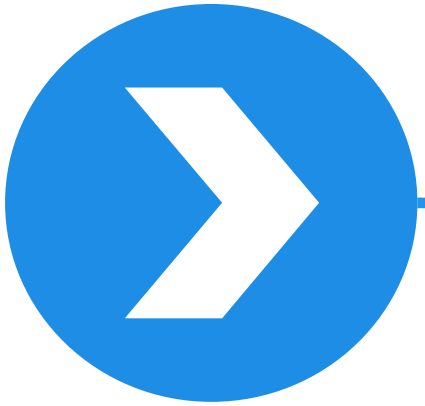
- 什么是ARK？
  - Anti-Rootkit
  - 小众工具，专业性强
- 什么是Rootkit?
  - Rootkit是一种特殊的恶意软件，它的功能是在安装目标上隐藏自身及指定的文件、进程和网络链接等信息，比较多见到的是Rootkit一般都和木马、后门等其他恶意程序结合使用。



认识Rootkit

- Rootkit是一种技术，这种技术有两个很重要的能力，也是很显著的特点：
  - 提权。root是unix/linux系统上超级用户，拥有最高的系统权限，广义上的root就是提权，如：*Android系统上的“一键root”就是这个目的。*
  - 隐藏。向用户界面隐藏自身，包括自身的进程、文件、网络连接等可被用户察觉的组件。

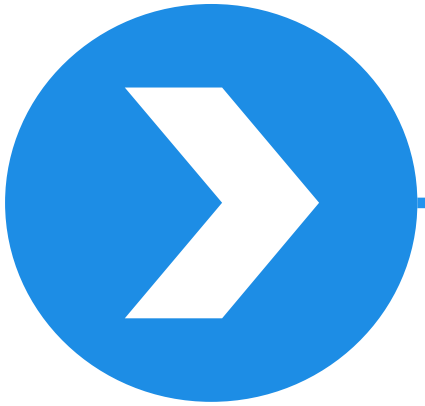
不是所有的恶意软件都叫Rootkit



Rootkit起源及威胁

- Rootkit源于unix/linux，兴于Windows，在XP时代达到顶峰
  - XP系统的普及，内核的弱安全性为Rootkit的发展提供了温床
  - 随着Vista、Windows7之后系统级安全级别的提高，内核PatchGuard的保护，对Rootkit的发展起到了遏制的作用
  - Rootkit的技术门槛被提高，不会消失

- Rootkit技术带来的威胁
  - 恶意软件配合Rootkit技术后，由于系统权限的提升，其攻击能力和隐蔽性也随之得到提升
  - 隐蔽性的提升增加检测和清除的难度，如传统反病毒软件无法感知到Rootkit的存在，因此容易漏扫
  - Rootkit表现得很顽强，反病毒软件束手无策的感觉



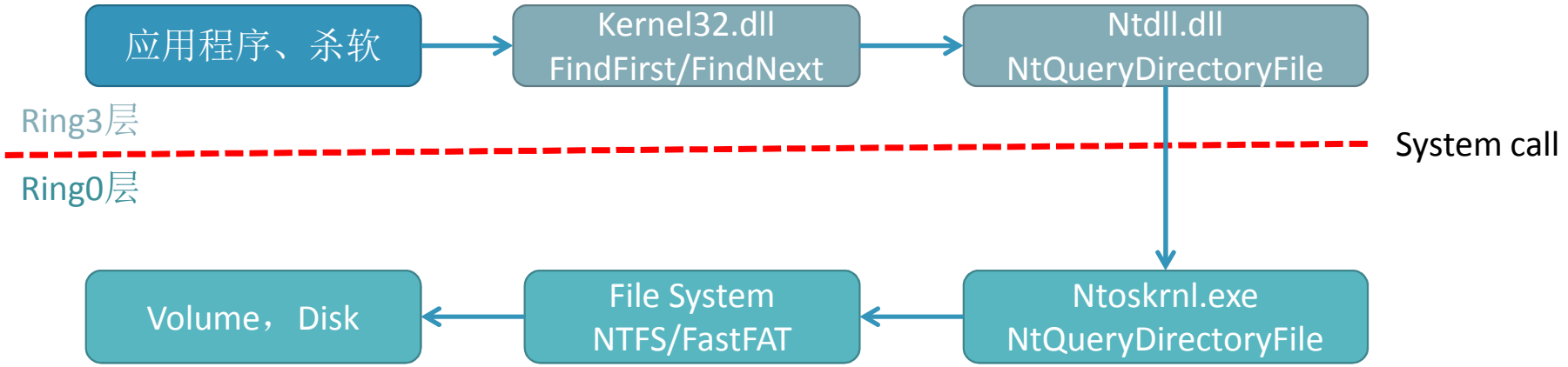
Rootkit的原理

- 知己知彼

- 它是怎么做到的？
  - 如何隐藏一个文件？

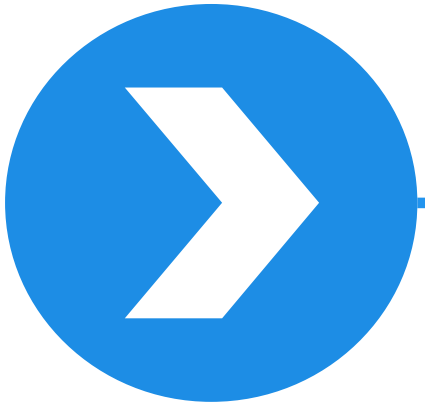
    隐藏是相对的，取决于你想对谁隐蔽

    如果相对于Windows应用软件，包括杀毒软件而言，遍历文件的过程是这样的



- 无处不在的HOOK
  - Windows系统上的Rootkit很大程度上得益于HOOK技术
  - HOOK的种类：inline hook，SSDT hook，IAT hook
  - HOOK得益于Windows内核的弱安全性：对驱动程序的完全信任
  - 微软支持HOOK，提供detours函数库帮助开发者实现
  - Windows模块支持 hotpatch 功能

- 利用HOOK技术进行攻击
  - 优先执行获取控制权
  - 系统级Rootkit使用驱动程序安装HOOK，应用级Rootkit使用全局钩子注入技术安装HOOK
  - 潜伏等待事件的触发，用来修改执行顺序或结果
  - 利用已经获取的宿主权限完成木马、后门、传播等恶意功能
  - 攻击破坏安防软件，如反病毒产品、防火墙等



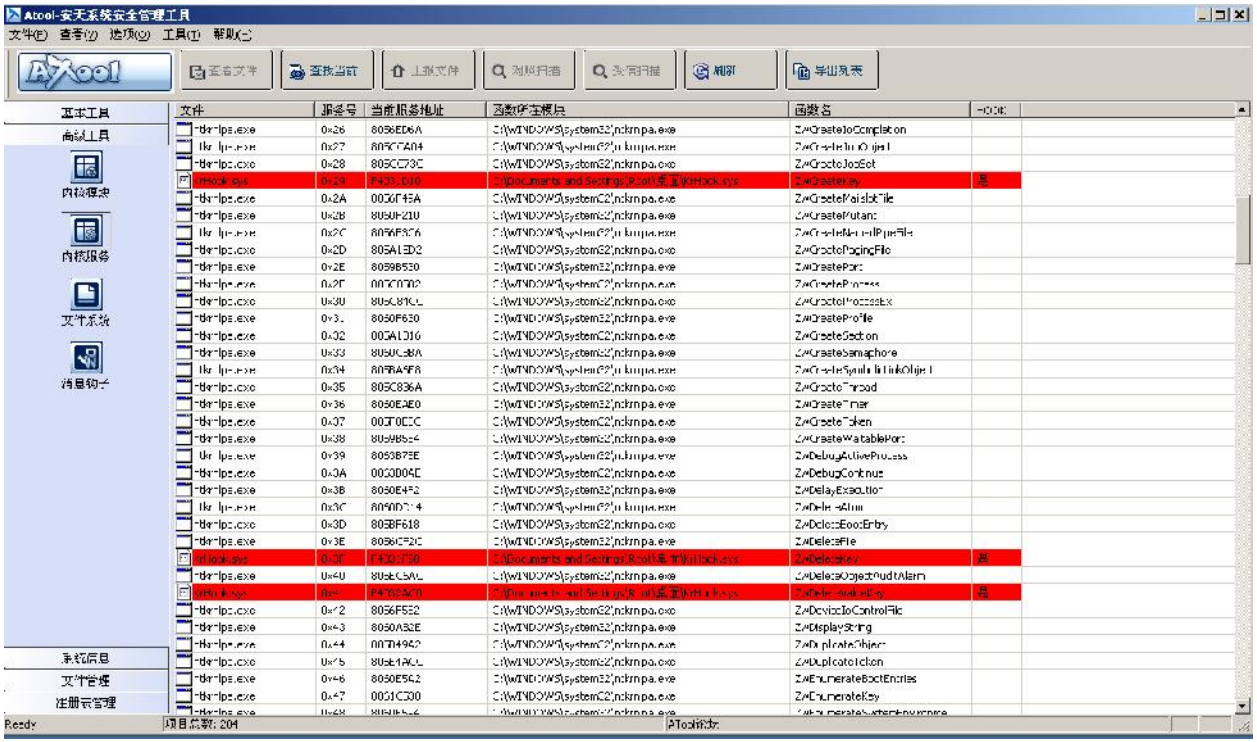
Anti-Rootkit的方法

- 获取真实的信息
  - 系统信息范围很大，包括我们熟知的：进程、文件、注册表、网络、服务、用户、共享等等
  - 系统信息的标准获取方式是 Windows API，在Rootkit入侵的情况下，这些API返回的信息可能不正确
  - 除了标准API,要获取正确的信息，还有两种候选的办法：一个是换个相关API的调用链间接获取，另一个是从内核更底层来获取
  - 后者是因为在API调用链上，只要比Rootkit的位置更低，就必然能获取真实的信息，深入的程度决定了开发的难度
  - 如何知道哪里调用更合适？

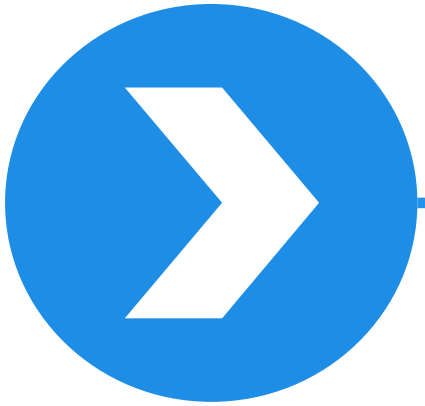
- 检测Rootkit钩子
  - 获取原始信息，从文件各个功能模块对应的原始程序文件中获取
  - 对于内核文件 ntoskrnl.exe 可以用来检测内核模块的变化，可以发现是否有篡改，一些比较常见的方法：
    1. 比较SSDT表的所有例程地址是否发生了变化，每个原始例程的入口代码是否发生了变化
    2. 比较SSDT表的子表是否发生了变化
    3. 比较所有引出函数的入口代码是否发生了变化

    同样的方法也适用于检测 win32k.sys 中的 SHADOW SSDT
  - 对于其它驱动程序，比如FSD，比较Dispatch例程的地址以及原始地址处的入口代码是否发生了变化
  - 一般检查的驱动包括：磁盘、网络、文件系统、键盘等
  - 对于应用层的模块：
    1. 遍历进程中的核心模块，并检查模块的引出函数入口代码是否发生了变化
    2. 检查进程引入表中所有模块的API地址是否被导向未知模块

- 检测Rootkit钩子
  - 这是一个用安天 ARK 工具atool检测到的SSDT钩子的案例，可以看到，SSDT钩子被清晰地标记出来了



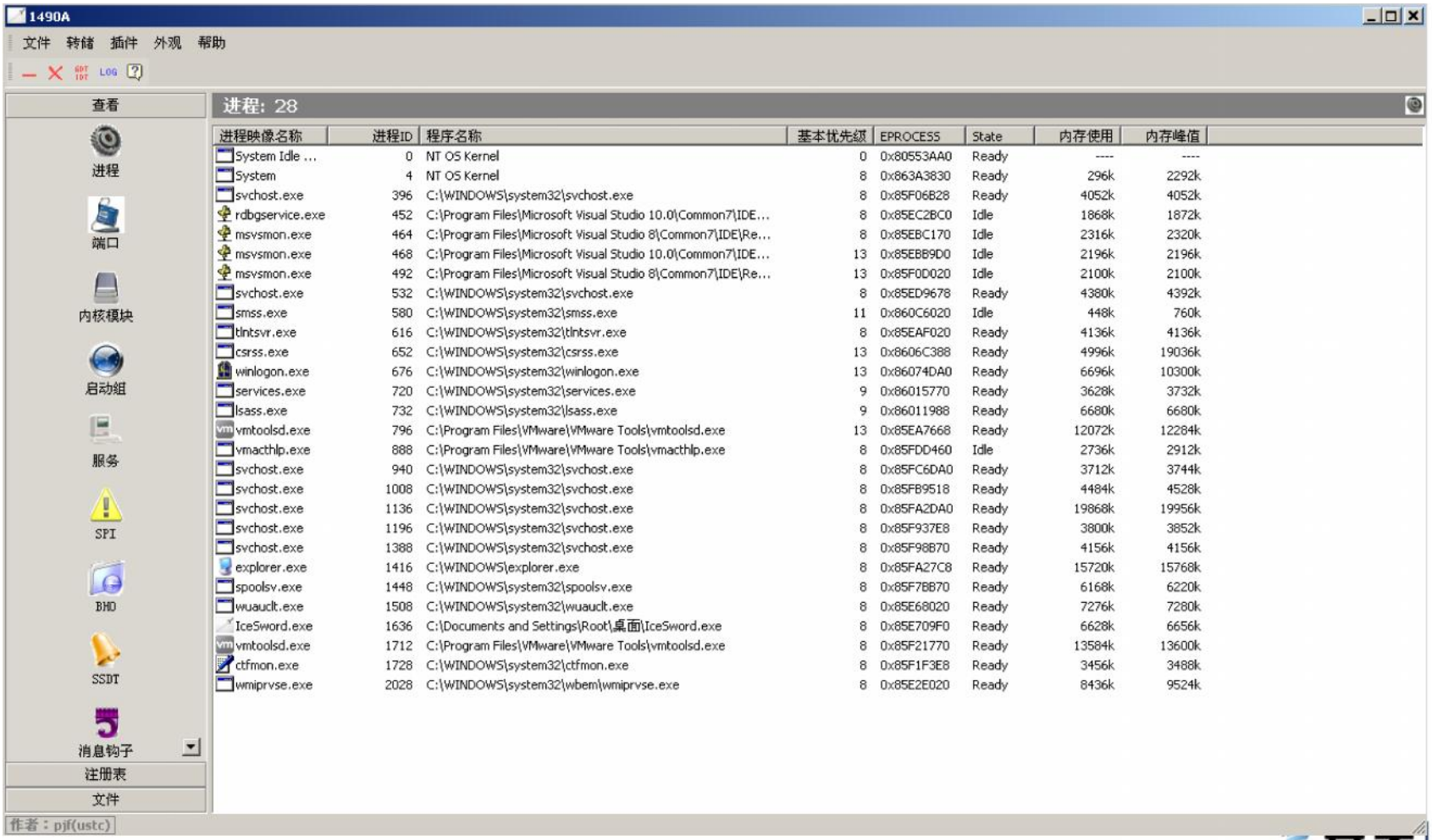
- 检测Rootkit
  - Rootkit并不总是要篡改系统内核，很多手段都是可以利用宿主系统提供的正式功能来完成，这一点在Windows和Linux系统中都存在可行性
  - 比如 Windows 系统的过滤驱动，各种回调接口等，如何枚举这些模块成为了检测的关键
  - 没有公开的方法揭示这些接口的内部数据结构，需要借助针对性的逆向分析
  - 即使了解数据结构，手工检测也几乎是不可能的，计算量太大



Anti-Rootkit工具

- Rootkit检测工具
  - Rootkit经常深入系统内核工作，涉及到大量的未公开数据结构，于是，一些自动分析检测的工具就产生了
  - 早期的ARK工具以清理Rootkit木马为主，这类木马通常比较顽强，不是普通的杀毒软件可以清除的，必须有功能强大的辅助工具来专杀，这时候的ARK工具在功能上以查看和清理为主
  - 查看的对象包括进程、文件、注册表项、网络端口、消息钩子等等，实现方法上以内核驱动程序为主，充分利用内核数据分析技术不但可以查看这些信息，还可以检测各种被隐藏项
  - 查看对象还可以还包括远离普通用户的那些专业技术信息，如内核模块、SSDT、服务等
  - 很重要的一点，可以查看那些散落在注册表各处的开机启动项，并可以任意清除它们

- Rootkit检测工具的清理功能
  - Rootkit检测还具有一定的清理功能，清理对象就是在检测过程中发现的异常项目
  - 比如各种HOOK（钩子），因为使用HOOK技术的性价比特别高，一来容易编写代码，二来功能非常强大，几乎可以完成许多正常手段做不到的事情，而且这些技术在XP上可以随心所欲不受系统限制，所以大家都爱用
  - Rootkit的大量涌现，必然会导致ARK工具的繁荣，这时期ARK工具出现了很多，基本以国产软件为主，其主要代表为IceSword(冰刃)，这款工具既可以暴露隐藏的进程、文件、注册表项还可以删除它们，最重要的是，它运行的相当稳定
  - 大部分的ARK工具对Rootkit的清除功能还不是很强大，仅限于删除文件、注册表，结束进程等常规功能的提升



- Rootkit检测工具的低落
  - 2007年时候，微次发布了XP的升级系统Vista，从用户角度看，这个新系统在安全性方面的最明显功能就是UAC，这个技术从多个方面对系统操作权限进行控制，以防止对系统关键部位的意外操作，具体地说，就是当某一程序需要较高的权限时，会提示用户，否则不能取得高权限
  - Vista同时也将数字签名技术正式引入到用户级应用程序中，通过界面差异让用户感觉到程序的可信性
  - Vista未能普及，Windows7开始登场，UAC访问权限控制系统被加强，变得更加易用，在这样的系统下，过去的Rootkit技术几乎不能获取系统级特权，甚至连开机自启动都难以做到了，迫使Rootkit升级，比如Bootkit
  - Bootkit通过感染MBR(磁盘主引记录）的方式，实现绕过内核检查和启动隐身，因为在开机时比Windows内核更早加载，很容易实现内核劫持的功能

- 国外的Rootkit检测工具
  - 不象反病毒产品等其它规模化正式发行的安全产品，ARK工具更象是单兵作战的利器，在国外安全技术领先的情况下，ARK工具发展的反而并不好，这表现在功能比较单一、信息挖掘不够深入、尤其缺乏国产工具那样直观手工清理的功能，缺少操控感，所在在国内并不盛行

- Rootkit检测工具的发展
  - Windows7之后，受系统安全性限制，Rootkit相对减弱，ARK工具的开发者们许多加入到了一些大公司麾下，市面上的ARK工具大多停止了更新，只有少数几个还在坚持，如Xuetr、PowerTool,Atool
  - Windows每升级一个版本，ARK工具都会减少一些，Windows10出现以后，特别是随着64位系统的普及，真正能用的只有PCHunter和安天的ATOOL了
  - 在x64平台上，由于Windows x64两个特性导致Rootkit开发遇到了瓶颈：一是对驱动程序强制要求交叉数字签名，这样Rootkit必须拥有有效的数字证书才可以，二是内核程序及关键数字的保护，不允许第三方修改，这样许许多多的Rootkit技术都不能使用了
  - 新一代的ARK工具不仅拓展了数据挖掘能力，也提升了威胁清除能力，可以查看内核更多更详细的数据结构，还能够麻利地清理或者还原异常数据，比如SSDT表，内核回调函数表等

- Rootkit检测工具的未来
  - Windows特别是64位系统的安全性增强，ARK工具越来越集中到极少数专业安全分析人员手中，对安全技术爱好者、发烧友而言，需求将会降低，取而代之的是功能更强、易用性更高的正式版安全产品
  - 这样看起来ARK工具的需求有所降低，实际上却是要求更高，只是侧重点会有所转变，比如文件来源分析，过去，几乎没有人关心电脑系统中的文件来自哪里，而现在这些信息可能是威胁检测的重要线索
  - 安全产业从业人员、技术分析人员仍然将依赖ARK工具进行协助分析，自身的定位和技术要求决定了ARK工具只会向功能更强、范围更广方面发展，对普通用户而言，仍然还是那么的难以理解
  - 安天作为一家反病毒引擎和解决方案厂商，提供检测PC恶意代码和移动恶意代码的顶级反病毒引擎和下一代反病毒服务，同时也持续提供新一代的ARK工具ATOOL供广大爱好者使用

谢谢大家

THANK YOU FOR YOUR ATTENTION