网络空间威胁对抗与防御技术研讨会
暨 第七届安天网络安全冬训营

威胁框架在端点主动防御和数据采集的应用

基于ATT&CK在端点防护的实践分享

安天端点安全产品子线

威胁框架：认知与实践

寒夜远征

寒夜远征

CONTENTS

目 录

01 威胁框架在端点防护的价值

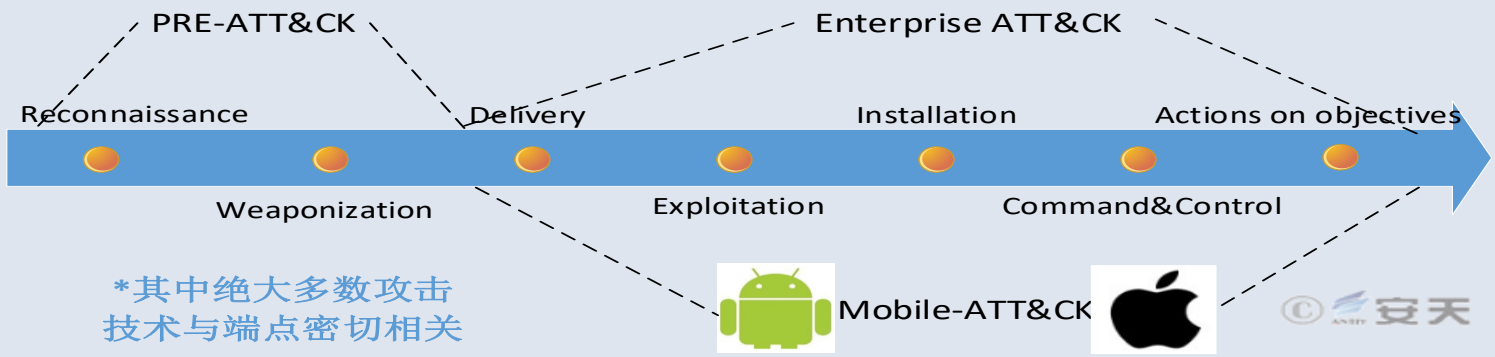
02 应用威胁框架提升主防和采集能力

03 实战案例解析与经验总结

01 威胁框架在端点防护的价值

端点是威胁对抗的主战场

杀伤链映射



*其中绝大多数攻击技术与端点密切相关

战术&技术选择

端点是攻击的主要落地点，遭受的攻击数量最多，同时敌方在"端点主战场"的投入最精良。以方程式组织在端点的作业链为例：

初始攻击	创建据点	提权	内部侦查	横向移动	持久存在	完成任务
传统APT手段	探测模块	获取令牌	获取系统信息	端口映射	进程隐蔽	键盘记录
介质投放	攻击插件与平台	修改用户组	获取网络信息	内部渗透	文件隐藏	文件窃取
物流链		修改安全策略	获取其他信息	远程执行	远程管理	密码窃取
人员带入		获取权限	共享枚举	网络嗅探	取证对抗	加密打包
				添加账号	连接隐蔽	下载执行
				摆渡攻击	注册表	账号窃取
					流量隐藏	结束进程
					固件植入	网络回传

*来源：安天发布的《方程式组织主机作业模块积木图》

端点防护作为防御的最后一道防线，应具有以下能力：

- ☑ 具有合理的架构安全体系，增强安全运维能力，以减少被攻击面。
- ☑ 具有足够纵深的主动防御能力，才能够在多个环节逐步抵消威胁。
- ☑ 具有全面的信息采集与分析能力，以便发现常规防御手段无法发现的威胁。

主动防御和数据采集在端点防护（EPP）中缺一不可

传统杀毒软件
（强主防、轻采集）

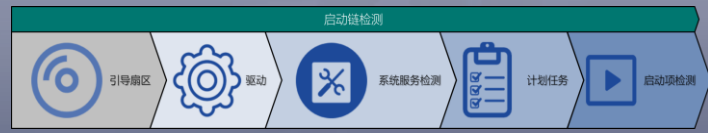
- 面对利用系统白文件的常规操作，如sc.exe、reg.exe等来完成攻击中信息搜集或持久化等过程，多数主防都不会判定为恶意。
- 某些0day漏洞，常规防御几乎无法感知，但可以通过关键数据采集发现异常现象，进而捕获威胁。
- 没有将防御动作作为数据进行采集记录的设计导向，使传统杀毒软件的主防能力并没有有效发挥。

端点防护平台

EPP（Endpoint Protection Platforms）是Gartner对端点防护产品的定义，它在传统杀软中增加了EDR技术，并在2018年将EDR从EPP的补充性功能变成必备功能。

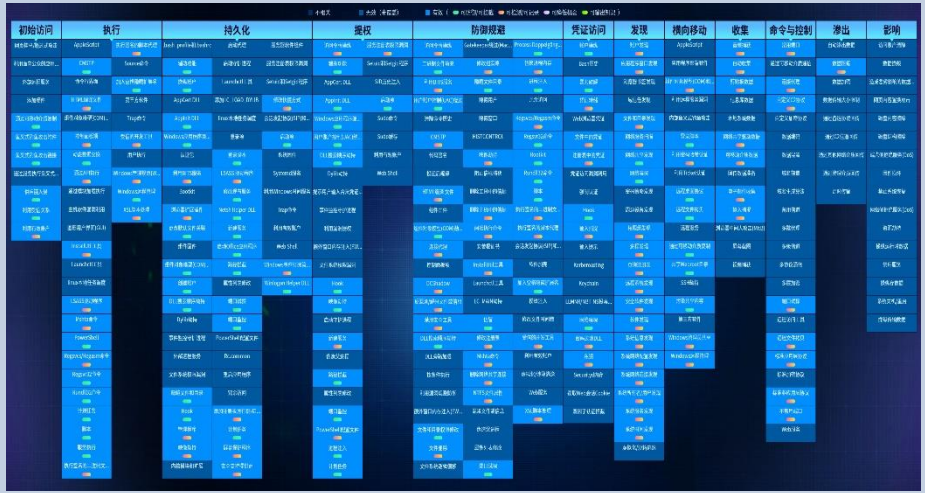
EDR类软件
（重采集、弱主防）

- 例如针对隐藏进程（T1014防御规避.Rootkit），基于主防是可以轻松感知和拦截的，但没有强主防技术基础的EDR基本上是无法发现的。EDR多数是基于应用层信息的提取，**无法获取系统级、驱动层的信息**，但往往这些数据才是支撑分析和画像最重要的依据。
- **EDR需要体系化的数据采集，以保证威胁发现的全面性。**例如针对添加自启动项，除了可以通过注册表实现外，还可以通过配置文件、计划任务等多种方式。



引入威胁框架可明显提升端点的防护和采集能力

威胁框架可以作为安全产品开发的可落地的参考及产品能力验证指标之一。



ATT&CK威胁框架可以帮助安全厂商对端点威胁有了更深入的认知，由**单载荷、单环节**的层面提升到**多个战术环节、多种攻击技术**的层面，由**被动防守的视角**转变为**以攻击者的视角**去理解威胁，使防御体系的构建更具有主动性。

单纯依靠载荷静态特征和已知恶意进程行为加权的方式，已无法全面感知威胁，说明数据（行为）采集需要足够的广度和深度，ATT&CK能够指导产品**构建清晰、完备的采集体系**，同时其相对统一的定义也有助于分析人员**快速准确、低成本**的进行威胁分析和协同工作。

威胁框架的落地，可以围绕主防能力在两个方向上发力

主防能力是威胁框架落地的基础

如果不具备强主防能力，针对很多ATT&CK技术点的防御是无从下手的。

在国内环境下，只有通过主防拦截了大量低层次的威胁，才能使我们聚焦于ATT&CK中高价值数据的采集。

寒夜速纪

威胁框架：认知与实践

02 如何应用威胁框架提升主防和采集能力

ATT&CK威胁框架在安天智甲终端防御系统的落地

智甲客户端主界面


智甲管理中心主界面

——产品定位——

智甲终端防御系统是安天研发的面向政企客户的**端点综合安全防护软件**，其内置**安天下一代威胁检测引擎**，为办公机、服务器、虚拟化节点、移动设备、国产专用计算机、各类自助终端、工控上位机等各类端点场景提供**多层次、全周期的动态防护能力**。

——功能、优势与价值——

核心功能

- 反病毒，包括病毒查杀、主动防御、威胁分析、威胁追溯与清除等；
- 终端管控，包括外设管控、运行管控、网络管控、白名单等。

产品优势

- 主动防御能力，尤其是针对勒索者、挖矿病毒等新兴威胁；
- 国产化防护方面具有领先优势，投入早、适配全，与全部主流国产化操作系统厂商达成兼容性互认证。

用户价值

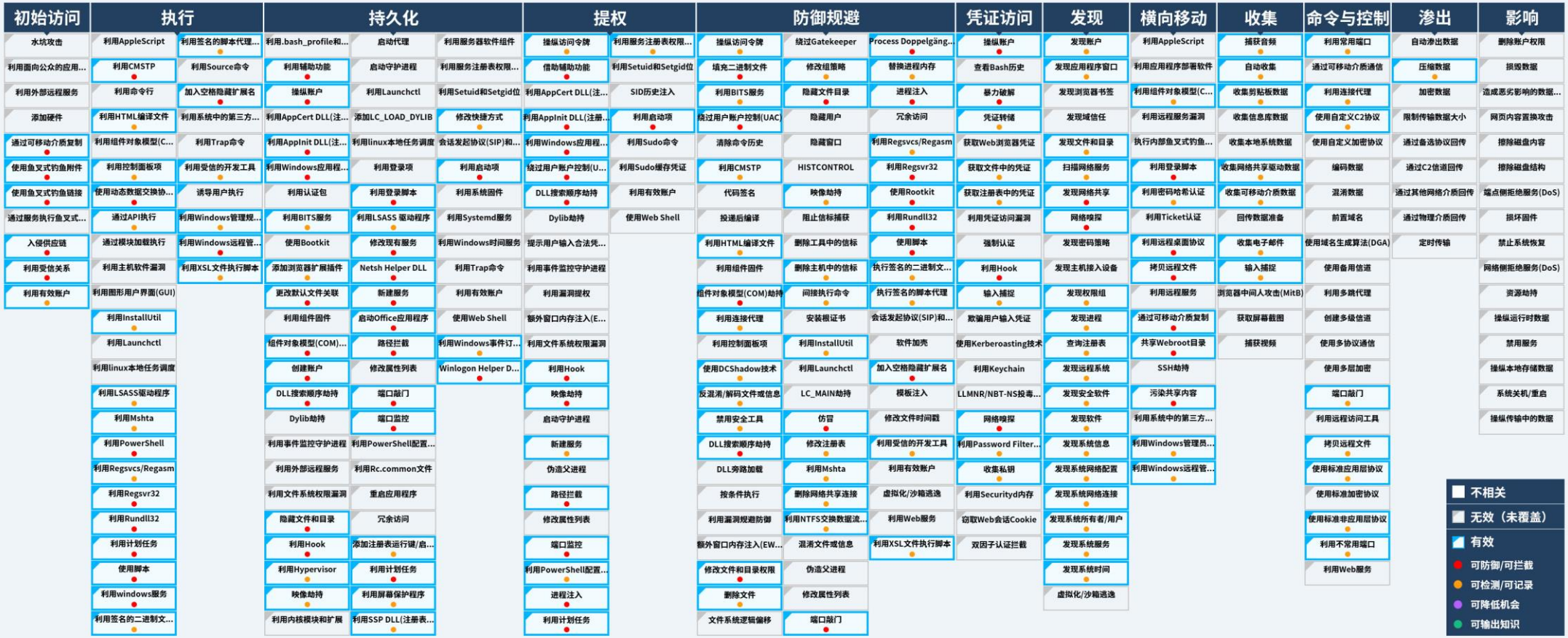
- 支持多种平台和不同类型终端的统一管理；
- 为威胁情报和态势感知提供重要的数据支撑。

典型安全事件所采用的攻击技术在ATT&CK中的映射

初始访问	执行		持久化			提权		防御规避			凭证访问	发现	横向移动	收集	命令与控制	渗出	影响
水坑攻击	利用AppleScript	利用签名的脚本代理...	利用.bash_profile和...	启动代理	利用服务器软件组件	操纵访问令牌	利用服务注册表权限...	操纵访问令牌	绕过Gatekeeper	Process Doppelgäng...	操纵账户	发现账户	利用AppleScript	捕获音频	利用常用端口	自动渗出数据	删除账户权限
利用面向公众的应用...	利用CMSTP	利用Source命令	利用辅助功能	启动守护进程	利用服务注册表权限...	借助辅助功能	利用Setuid和Setgid位	填充二进制文件	修改组策略	替换进程内存	查看Bash历史	发现应用程序窗口	利用应用程序部署软件	自动收集	通过可移动介质通信	压缩数据	损毁数据
利用外部远程服务	利用命令行	加入空格隐藏扩展名	操纵账户	利用Launchctl	利用Setuid和Setgid位	利用AppCert DLL(注...	SID历史注入	利用BITS服务	隐藏文件目录	进程注入	暴力破解	发现浏览器书签	利用组件对象模型(C...	收集剪贴板数据	利用连接代理	加密数据	造成恶劣影响的数据...
添加硬件	利用HTML编译文件	利用系统中的第三方...	利用AppCert DLL(注...	添加LC_LOAD_DYLIB	修改快捷方式	利用AppInit DLL(注册...	利用启动项	绕过用户账户控制(UAC)	隐藏用户	冗余访问	凭证转储	发现域信任	利用远程服务漏洞	收集信息库数据	使用自定义C2协议	限制传输数据大小	网页内容置换攻击
通过可移动介质复制	利用组件对象模型(C...	利用Trap命令	利用AppInit DLL(注...	利用linux本地任务调度	会话发起协议(SIP)和...	利用Windows应用程...	利用Sudo命令	清除命令历史	隐藏窗口	利用Regsvcs/Regasm	获取Web浏览器凭证	发现文件和目录	执行内部鱼叉式钓鱼...	收集本地系统数据	使用自定义加密协议	通过备选协议回传	擦除磁盘内容
使用鱼叉式钓鱼附件	利用控制面板项	利用受信的开发工具	利用Windows应用程...	利用登录项	利用启动项	绕过用户账户控制(U...	利用Sudo缓存凭证	利用CMSTP	HISTCONTROL	利用Regsvr32	获取文件中的凭证	扫描网络服务	利用登录脚本	收集网络共享驱动数据	编码数据	通过C2信道回传	擦除磁盘结构
使用鱼叉式钓鱼链接	使用动态数据交换协...	诱导用户执行	利用认证包	利用登录脚本	利用系统固件	DLL搜索顺序劫持	利用有效账户	代码签名	映像劫持	使用Rootkit	获取注册表中的凭证	发现网络共享	利用密码哈希认证	收集可移动介质数据	混淆数据	通过其他网络介质回传	端点侧拒绝服务(DoS)
通过服务执行鱼叉式...	通过API执行	利用Windows管理规...	利用BITS服务	利用LSASS 驱动程序	利用Systemd服务	Dylib劫持	使用Web Shell	投递后编译	阻止信标捕获	利用Rundll32	利用凭证访问漏洞	网络嗅探	利用Ticket认证	回传数据准备	前置域名	通过物理介质回传	损坏固件
入侵供应链	通过模块加载执行	利用Windows远程管...	使用Bootkit	修改现有服务	利用Windows时间服务	提示用户输入合法凭...		利用HTML编译文件	删除工具中的信标	使用脚本	强制认证	发现密码策略	利用远程桌面协议	收集电子邮件	使用域名生成算法(DGA)	定时传输	禁止系统恢复
利用受信关系	利用主机软件漏洞	利用XSL文件执行脚本	添加浏览器扩展插件	Netsh Helper DLL	利用Trap命令	利用事件监控守护进程		利用组件固件	删除主机中的信标	执行签名的二进制文...	利用Hook	发现主机接入设备	拷贝远程文件	输入捕捉	使用备用信道		网络侧拒绝服务(DoS)
利用有效账户	利用图形用户界面(GUI)		更改默认文件关联	新建服务	利用有效账户	利用漏洞提权		组件对象模型(COM)劫持	间接执行命令	执行签名的脚本代理	输入捕捉	发现权限组	利用远程服务	浏览器中间人攻击(MitB)	利用多跳代理		资源劫持
	利用InstallUtil		利用组件固件	启动Office应用程序	使用Web Shell	额外窗口内存注入(E...		利用连接代理	安装根证书	会话发起协议(SIP)和...	欺骗用户输入凭证	发现进程	通过可移动介质复制	获取屏幕截图	创建多级信道		操纵运行时数据
	利用Launchctl		组件对象模型(COM)...	路径拦截	利用Windows事件订...	利用文件系统权限漏洞		利用控制面板项	利用InstallUtil	软件加壳	使用Kerberoasting技术	查询注册表	共享Webroot目录	捕获视频	使用多协议通信		禁用服务
	利用linux本地任务调度		创建账户	修改属性列表	Winlogon Helper D...	利用Hook		使用DCShadow技术	利用Launchctl	加入空格隐藏扩展名	利用Keychain	发现远程系统	SSH劫持		使用多层加密		操纵本地存储数据
	利用LSASS驱动程序		DLL搜索顺序劫持	端口敲门		映像劫持		反混淆/解码文件或信息	LC_MAIN劫持	模板注入	LLMNR/NBT-NS投毒...	发现安全软件	污染共享内容		端口敲门		系统关机/重启
	利用Mshta		Dylib劫持	端口监控		启动守护进程		禁用安全工具	仿冒	修改文件时间戳	网络嗅探	发现软件	利用系统中的第三方...		利用远程访问工具		操纵传输中的数据
	利用PowerShell		利用事件监控守护进程	利用PowerShell配置...		新建服务		DLL搜索顺序劫持	修改注册表	利用受信的开发工具	利用Password Filter...	发现系统信息	利用Windows管理员...		拷贝远程文件		
	利用Regsvcs/Regasm		利用外部远程服务	利用Rc.common文件		伪造父进程		DLL旁路加载	利用Mshta	利用有效账户	收集私钥	发现系统网络配置	利用Windows远程管...		使用标准应用层协议		
	利用Regsvr32		利用文件系统权限漏洞	重启应用程序		路径拦截		按条件执行	删除网络共享连接	虚拟化/沙箱逃逸	利用Securityd内存	发现系统网络连接			使用标准加密协议		
	利用Rundll32		隐藏文件和目录	冗余访问		修改属性列表		利用漏洞规避防御	利用NTFS交换数据流...	利用Web服务	窃取Web会话Cookie	发现系统所有者/用户			使用标准非应用层协议		
	利用计划任务		利用Hook	添加注册表运行键/启...		端口监控		额外窗口内存注入(EW...	混淆文件或信息	利用XSL文件执行脚本	双因子认证拦截	发现系统服务			利用不常用端口		
	使用脚本		利用Hypervisor	利用计划任务		利用PowerShell配置...		修改文件和目录权限	伪造父进程			发现系统时间			利用Web服务		
	利用windows服务		映像劫持	利用屏幕保护程序		进程注入		删除文件	修改属性列表			虚拟化/沙箱逃逸					
	利用签名的二进制文...		利用内核模块和扩展	利用SSP DLL(注册表...		利用计划任务		文件系统逻辑偏移	端口敲门								

ATT&CK技术点对应的危害等级

安天智甲对ATT&CK威胁框架的覆盖度



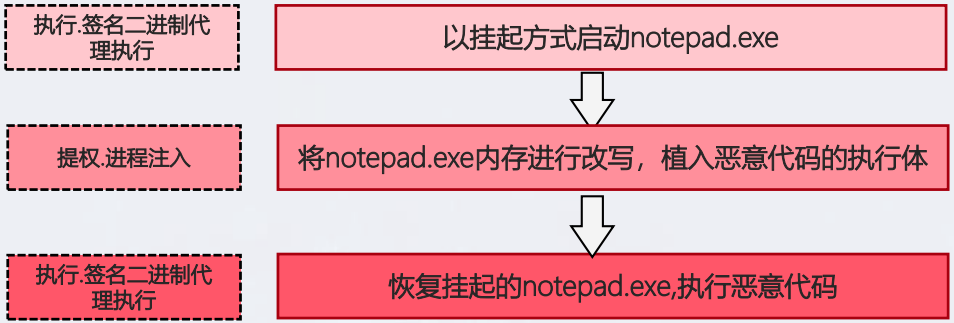
智甲主防各类防御点在ATT&CK的映射

ATT&CK在端点侧的落地需要完备的主防能力

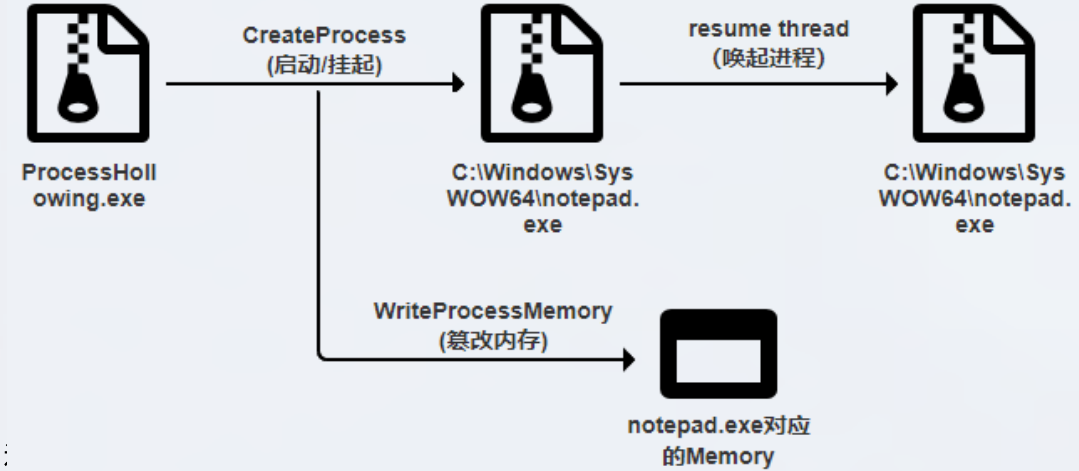
步骤	攻击动作	对应的ATT&CK技术点	ATT&CK提供的防御方法	安天智甲防御规则
01	使用钓鱼邮件，邮件中包含宏病毒，传统杀软无法检测	T1193初始访问.鱼叉式钓鱼附件 T1192初始访问.鱼叉式钓鱼攻击链接 T1199初始访问.利用受信关系	**仅描述了防护的思路** （没有防护方法）	防御方式：邮件监控 防护策略：邮件正文监控，接收附件是否存在敏感词汇、诱饵名称、钓鱼链接、钓鱼附件等
02	利用宏病毒执行Rundll32加载前导DLL实现提权	T1173执行.动态数据交换 T1085执行.Rundll32命令	**仅描述了防护的思路** （没有office启动系统文件的防护方式）	防御方式：进程监控 防护策略：采集office文档启动 PE文件，采集Rundll32加载DLL执行
03	创建系统服务实现持久化并释放rootkit驱动，实现隐藏文件、进程和服务	T1050提权.新建服务 T1158持久化.隐藏文件和目录 T1158防御规避.隐藏文件和目录	使用命令行参数执行防护 **（防护方式不足，没有涵盖API方式）**	防御方式：注册表监控、文件监控、进程监控 防护策略：检测是否存在危险行为，包括非法第三方应用建立服务和驱动、修改PE文件属性为隐藏、进程隐藏等
04	服务启动后，执行窃取用户信息，并回连	T1033发现.发现系统所有者/用户	使用命令行参数执行防护 **（防护方式不足，没有涵盖API方式）**	防御方式：敏感程序监控、敏感API调用监控 防御策略：采集系统常用命令执行，并记录详细的操作信息；采集敏感API调用，并记录详细操作信息
05	利用移动设备，感染移动介质生成autorun.inf，关联rundll32启动前导DLL，并文件属性为隐藏，继续扩散	T1158持久化.隐藏文件和目录 T1091横向移动.通过可移动介质复制	**仅描述了防护的思路** （没有防护方法）	防御方式：移动存储设备监控 防御策略：监控并检测移动存储设备环境变化，包括文件改变、出现autorun.inf、修改PE文件属性为隐藏
06	定时向内网横向移动，最终达到缓慢扩散	T1110凭证访问.暴力破解	本地命令行撞库方法 **（没有提及网络破解方法）**	防御方式：网络防护 防御策略：检测是否存在高频内网敏感端口发送数据

在ATT&CK的基础上提升主防能力

某些恶意代码会将执行体写入正常进程的内存中（通常是系统程序或者常见的应用程序），以此实现绕过主动防御或者EDR产品的数据采集与监控。



ATT&CK将其定义为Process Hollowing技术，**但认为该类攻击无法通过事前预防性控制来缓解。**基于此指引，智甲将重点放在**事中防御与事后防御。**



防御策略1（事中防御）：通过数据采集功能监测CreateProcess事件的详情，并同时监控VirtualAllocEx、WriteProcessMemory、GetThreadContext、SetThreadContext、ZwUnmapViewOfSection等**多个关键API，在发现内存篡改行为后立即进行拦截和告警。**

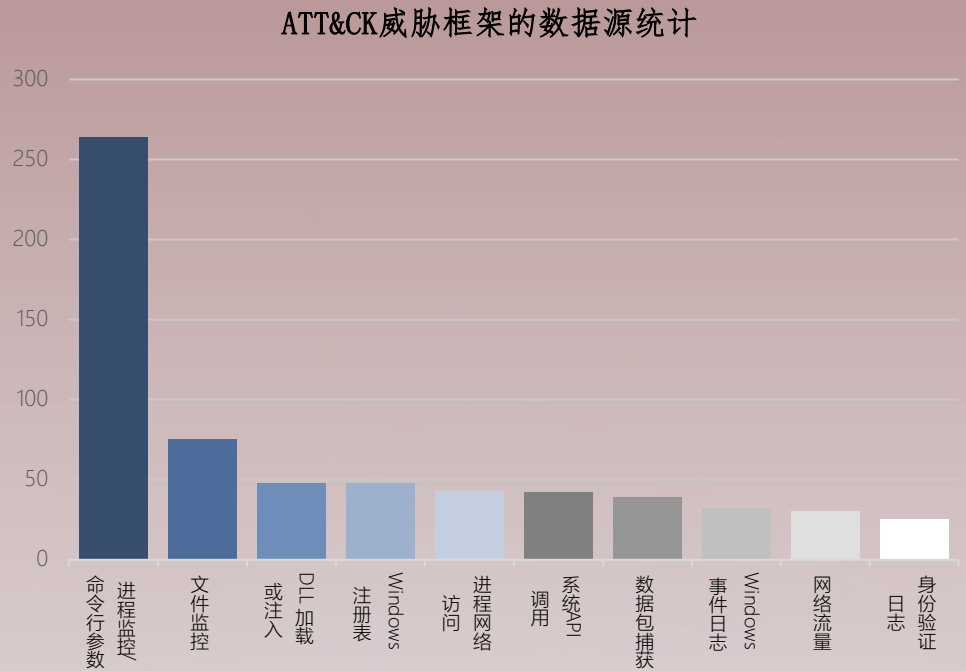
防御策略2（事后防御）：如果在安装系统前用户终端已遭到该类攻击，可以在安装系统后**对所有存活进程的内存进行扫描，并将该内存与存储在磁盘中的实体进行匹配，**当发现内容不匹配后，会主动分析其不匹配原因，查看是否挂钩或者进行相应的内存修改，如果**发现恶意代码会主动结束恶意程序的执行。**

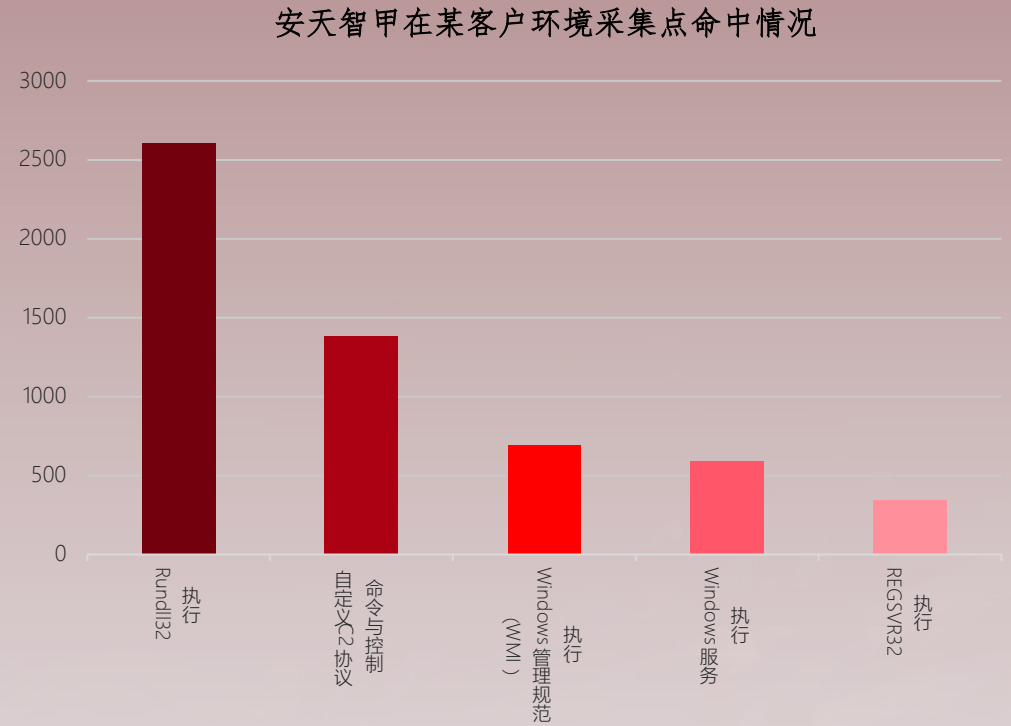
基于ATT&CK技术点中的数据源完善智甲的采集能力

类型	进程监控	文件监控	网络监控	系统信息	日志信息
既有	进程监控 DLL加载或注入 WMI对象 二进制文件元数据 服务监控 进程网络访问 浏览器扩展 内核驱动程序	MBR信息 文件监控 网络共享信息	邮件监控 网络流量 数据包捕获 网络入侵检测系统 网络协议分析 主机网络接口	Windows注册表 资产管理	系统日志 Web日志
新增	进程命令行参数 利用防病毒 命名管道 系统调用 内存发现异常HOOK 系统API调用				密钥文件访问日志
额外				Wi-Fi连接信息 漏洞信息 账号与口令	USB设备使用

防御和采集是一体的，所有主防的防御动作都可以根据配置决定是否记录

从两个维度看采集点





- 在做端点侧数据采集和分析时，应对进程类信息投入更多资源
- 主机防火墙在信息采集中意义重大
- 全要素采集量是巨大的，能够为不同场景配置不同的采集策略才能更好的落地

不同应用场景下的数据采集方案

	日常监控	重点蹲守	处置追溯
监控项目	重点监控关键项目，包括进程信息、文件信息、漏洞信息等	全项目监控，除常规项目外，关注**内存发现异常HOOK、系统API调用等**	主要采集特定文件传播情况，或者**网络流向情况等横向传播环节相关**数据进行采集
采集方式	产品默认采集范围	除默认采集外，针对特定范围端点进行全要素采集	自定义规则，按需采集
数据处理方式	管理人员重点关注告警信息即可	不仅对告警，还要对可疑事件进行关注	关注数据传播过程和途径
注意事项	保障系统性能与运行稳定性	重点监控目标，尽量不留死角	尽量实现在内网终端间的攻击线路还原

ATT&CK对端点数据采集能力的增益

可作为攻击事件的回溯依据

- 更全面的记录端点环境变更历史，包括文件新增情况、进程行为、注册表变化等，提供溯源依据；
- 通过将攻击事件中使用的攻击技术映射到ATT&CK，更好的理解对手的TTPs。

聚焦更重要的数据

- 针对攻击手段可能留下的数据痕迹，例如用户登录、外设文件利用等，进行专项采集；
- 针对系统组件被恶意利用，如Regsvr32.exe、PowerShell调用等，加强数据采集。

为态势感知提供数据支持

- 提供的数据类型更多，例如系统敏感API调用等，可以更好的进行分析威胁；
- 提供的数据信息更全，例如不止是病毒名称，更包括各种行为信息，可以更好地进行威胁研判。

寒夜速记

威胁框架：认知与实践

03 实战案例解析与经验总结

安天智甲融合威胁框架后获得的增益

战术环节	攻击动作	攻击技术	输出标签	防御技术
初始访问	接收恶意邮件	模拟单位邮箱，发送钓鱼邮件	T1193鱼叉式钓鱼附件	用户接收附件时 检测附件
执行	诱导用户执行附件	附件利用rar软件CVE-2018-20252漏洞，执行恶意代码	T1064脚本	检测邮件附件是否 包含SFX文件
	写入磁盘	利用rar软件CVE-2018-20252漏洞，执行恶意代码	无	文件防御，解压时释放文件到启动目录，检测该文件
防御规避	利用诱饵文件名，诱导用户主动执行，绕过UAC验证	利用诱饵文件名，诱导用户主动执行，绕过UAC验证	T1204用户执行 T1088绕过用户帐户控制	进程防御，EXPLORER启动文件时对启动文件进行检测
发现	运行后，枚举操作系统和软件	查询系统操作系统和已经安装的软件	T1124系统时间发现 T1082系统信息发现	监控系统敏感API调用，包括：GetSystemInfo、GetSystemTime
	枚举账户和权限	查询系统当前用户信息	T1033系统所有者/用户发现	监控 系统敏感API调用，GetUserName
凭证访问	获得用户名密码凭证	执行powershell 脚本获取lsass.exe进程中当前系统的用户名和密码	T1003凭证转储	进程监控，PowerShell执行参数检测，脚本文件检测
横向移动	通过SMB漏洞横向移动	采用CVE-2017-0143 永恒之蓝SMB远程服务漏洞进行横向扩散	T1021远程服务	网络链接监控，敏感端口向内网高频横向扩散行为检测，敏感端口向本机恶意入侵检测
持久化	写入注册表启动项	达到持久化目的	T1060注册表运行键值/启动文件夹	创建启动项检测
凭证访问	记录键盘	通过键盘钩子实现键盘记录	T1179 Hooking	内存存在异常钩子
命令控制	与服务端回连	客户端和服务端每45s会进行一次tcp连接，并持续交互指令信息，其中流量数据均加密	T1071标准应用层协议 T1022数据加密	进程联网情况检测
	执行远程指令	与服务端交互指令，并执行指令	T1094自定义命令和控制协议	CMD执行命令及参数

攻击者操作

分析师可以结合红色部分的信息，发现上述威胁

安天智甲处置

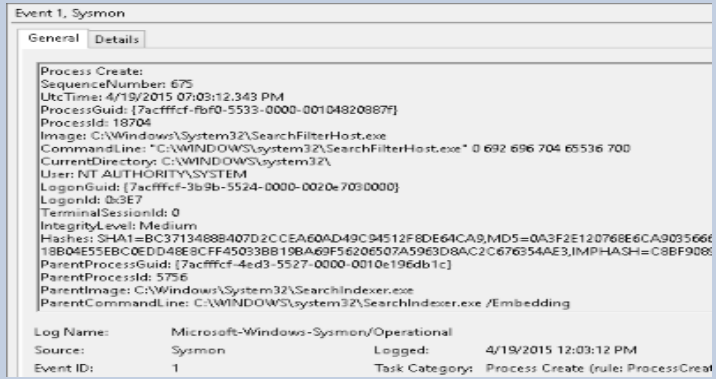
威胁框架落地的经验总结

ATT&CK不能仅用于对分析报表的丰富，要避免成为当年"初代"态势感知只有"地图炮"的情况

ATT&CK的最初实现图

安全产品更多需要具有原生的主防和采集能力，而不要过度依赖第三方工具

- 如果过于依赖Sysmon等第三方监控工具，既没有完成产品自身能力的闭环，也对威胁情报等安全资源利用效率造成障碍；
- 工具类（仍以Sysmon为例）的不可持续性不适合企业级常态化监控场景，其配置的复杂度也不具备在规模化端点环境下的实施条件。



Sysmon

威胁框架在端点侧的展望

从ATT&CK中针对端点的攻击手段占据了较大比重来看，端点是网络攻防战中的主战场。尤其是在面对高威胁对抗的网络攻击时，边界侧的防护能力正在逐渐失效，因此未来应当在**端点侧投入**更多努力以提升主动防御和数据采集能力。

威胁框架使我们对端点主动防御和数据采集的能力指标有了更清晰认知和衡量标准。我们可以通过威胁框架去**检验端点防御能力**和**采集范围**的有效性，并加以完善。

威胁框架不是全面的囊括，需要持续探究**现有威胁框架没有覆盖**的攻击手段。

- 横向上不断提升在各个攻击环节的覆盖面
- 纵向上加深对各攻击点的研究与防护投入
- 落地为适合国内环境的最佳实践

谢谢大家