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
Drive-by Compromise，如水坑攻击	计划任务			文件填充	网络嗅探		AppleScript（macOS系统）	音频捕获	常用端口	利用脚本收集和过滤数据	销毁数据，如反取证
利用联网的程序或服务的漏洞，如网站、SSH	Launchctl（macOS系统）		操作访问令牌		账户操作，如Mimikatz	账户枚举	应用部署软件，如McAfee ePO	自动收集，如使用脚本批量操作	使用可移动介质通信	数据压缩	加密数据
	计划任务，如at、cron		绕过UAC		Bash History	应用程序窗口枚举		系统粘贴板		数据加密	“ 恶作剧 ”
外部远程访问服务，如VPN	LSASS Driver/lsass.exe		Extra Window Memory注入		暴力破解		DCOM，如Empire利用Invoke-DCOM利用远程COM执行进行横向移动	信息存储库中的数据，如SharePoint	连接代理，如SOCK5	数据传输大小限制	覆写数据
物理渗透硬件，如Hak5 Wi-Fi Pineapple	Trap命令		进程注入		凭证转储	浏览器书签枚举			使用自定义 “ 命令和控制 ” 协议	通过其他网络媒体渗出，如蓝牙	擦除硬盘数据
通过可移动介质传播	AppleScript（macOS和OS X系统）	DLL搜索劫持			文件中的凭证，如SAM文件		远程服务的漏洞利用，如APT28利用Windows SMB远程执行代码漏洞进行横向移动	本地系统中的数据			主机拒绝服务
	CMSTP（微软连接管理器配置文件安装程序）	映像劫持（IFEO）			注册表中的凭证	域信任枚举		网络共享驱动器中的数据	使用自定义加密协议，如RTM用一个自定义的RC4变量来加密C2通信。	通过C2信道回传	损坏固件，如刷BIOS
带有附件的鱼叉式钓鱼邮件	命令行界面	修改Plist（macOS系统）			利用认证机制缺陷	文件和目录枚举	登录脚本				破坏 “ 系统恢复 ” 功能
带有恶意链接的鱼叉式钓鱼邮件	.chm格式文件	账户操作				网络服务枚举	Pass the Hash	可移动介质中的数据，如USB	数据编码	通过非C2信道回传	网络拒绝服务
利用第三方服务进行网络钓鱼	Windows控制面板项	辅助功能，如utilman.exe		BITS（后台智能传输服务）	强制认证，如强制SMB身份验证访问用户帐户哈希	网络共享枚举	Pass the Ticket	暂存数据	数据混淆		降低性能
（软件）供应链入侵	动态数据交换（DDE）协议	利用AppCert DLLs		清除命令历史记录	Hooking	密码策略枚举	RDP远程桌面	电子邮件	域前置(Domain Fronting)	通过物理介质渗出	运行时数据操作
受信任的关系，如受信任的第三方	通过API执行，如CreateProcessA()	利用AppInit DLLs		CMSTP（微软连接管理器配置文件安装程序）	输入捕获	外围设备枚举	远程文件复制，如scp	输入捕获	DGA算法		停止或禁用服务
合法账号	通过模块加载执行，如LoadLibraryExW()	Application Shimming（Microsoft Windows应用程序兼容性框架）		代码签名	输入提示	权限组枚举	远程服务，如SSH	浏览器中间人		有计划的传输	修改数据
		Dylib劫持（macOS系统）		.chm格式文件	Kerberoasting（一种Kerberos活动目录攻击方法）	进程枚举	通过可移动介质进行复制	屏幕捕获	备用信道		传输数据操作，如LightNeuron能够在传输过程中修改电子邮件内容。
	客户端执行的利用，如WinRAR	文件系统权限设置不当		组件固件，如硬盘固件	Keychain（macOS 钥匙串）	查询注册表		视频捕获	多阶段通信		
		Hooking		COM劫持	LLMNR/NBT-NS欺骗攻击	远端系统枚举	共享Webroot		使用多层代理		
	图形用户界面	Launch Daemon（macOS系统）				安全软件枚举	SSH劫持		使用多层加密		
	InstallUtil命令行实用程序	新增服务		Windows控制面板项	Password Filter DLL	系统信息枚举	感染网络共享文件		多级通道		
	Mshta，执行HTA的实用程序	路径拦截		DCShadow（针对活动目录）	私钥		第三方软件，如SCCM		Port Knocking		
	PowerShell	端口监视器		编码的文件或信息	Securityd内存（macOS系统）	系统网络配置枚举	Windows管理共享，如C$		远程访问工具		
	Regsvcs/Regasm	服务注册表权限设置不当			双因素身份验证拦截		Windows远程管理（WinRM）		远程文件复制		
	Regsvr32	Setuid 和 Setgid		禁用安全产品或工具		系统网络连接枚举			标准应用层协议		
	Rundll32	系统启动时自动加载		DLL Side-Loading，如绕过UAC							
	解释脚本，如APT1使用批脚本自动执行命令	Web Shell		Execution Guardrails（根据环境调整行为）		所有者/用户枚举			使用标准加密		
	服务执行，如net start/stop	.bash_profile 和 .bashrc	操作系统漏洞利用 应用程序漏洞利用	防御规避漏洞利用，如利用反病毒软件的漏洞							
	使用具有数字签名的程序代理执行，如Msiexec.exe	账户操作，如APT3将创建的帐户添加到本地管理组				系统服务枚举			标准非应用层协议，如SOCKS、raw socket		
		Windows身份验证包（身份验证包由LSA进程在系统启动时加载）	SID-History 注入	删除文件		系统时间枚举					
	使用具有数字签名的脚本代理执行，如APT32使用微软签名的pubprn.vbs来执行恶意软件	BITS（后台智能传输服务）	Sudo	修改文件权限					不常用端口		
		Bootkit	Sudo缓存			虚拟化/沙箱枚举			Web Service，如Dropbox和C2		
	Source命令	浏览器扩展		文件系统逻辑偏移量，如绕过文件系统访问控制							
	文件名后的空格	修改文件类型关联		绕过Gatekeeper（macOS系统）							
	第三方软件，如SCCM			修改组策略							
	受信的开发工具，如WinDbg、MSBuild	组件固件，如硬盘固件		隐藏文件和目录							
	用户执行,如用户打开钓鱼邮件的附件	COM劫持		隐藏用户							
	WMI			隐藏窗口							
		新增账户		HISTCONTROL环境变量，跟踪history命令应保存的内容							
	Windows远程管理（WinRM）	外部远程访问服务，如VPN		阻止主机信标上传							
		隐藏文件和目录		Indicator Removal from Tools，如免杀							
	XSL脚本处理	安装Hypervisor Rootkit		清理主机痕迹，如Bash History							
		内核模块和扩展，如内核模式Rootkit		间接命令执行，如使用Forfiles执行命令避免使用CMD							
		Launch Agent（macOS系统）		安装根证书							
		LC_LOAD_DYLIB （macOS系统）		InstallUtil命令行实用程序							
		登录项（macOS系统）		Launchctl（macOS系统）							
		使用登录脚本		LC_MAIN劫持（macOS系统）							
		修改现有服务		伪装，如将psexec服务名改为mstdc							
		使用Netshell执行恶意DLL		修改注册表							
		利用Office程序启动		Mshta，执行HTA的实用程序							
		Port Knocking		移除网络共享[记录]							
		Rc.common（macOS系统启动时会执行此脚本）		NTFS文件属性，如Alternate Data Streams							
		Redundant Access		混淆的文件或信息							
		注册表运行项/启动文件夹		Port Knocking							
		利用macOS系统重新打开的应用程序特性		Process Doppelgänging代码注入技术							
		屏幕保护程序		Process Hollowing，类似于进程注入							
		Windows安全支持提供程序（SSP）		Redundant Access							
		修改快捷方式，如LNK劫持		Regsvcs/Regasm							
		SIP和信任提供程序劫持		Regsvr32							
		系统固件		Rootkit							
		Systemd服务（Linux）		Rundll32							
		时间提供程序		解释脚本							
		WMI 事件订阅		使用具有数字签名的程序代理执行，如Msiexec.exe							
		Winlogon		使用具有数字签名的脚本代理执行，如APT32使用微软签名的pubprn.vbs来执行恶意软件							
				SIP和信任提供程序劫持							
				软件打包							
				文件名后的空格							
				模板注入(Office文件)							
				Timestomp，修改文件时间戳							
				受信的开发工具，如WinDbg、MSBuild							
				反虚拟化/沙箱							
				Web Service，如Twitter用作C2							
				XSL脚本处理							

MITRE ATT&CK™ Enterprise Framework

attack.mitre.org

MITRE ATT&CK™ Enterprise Framework中译版

By：Zer0d0y@天御攻防实验室

MITRE