威胁框架的发展与深化

安天研究院

前言

2020.1

ATT&CK®

2021.1

MITRE

长缨待展

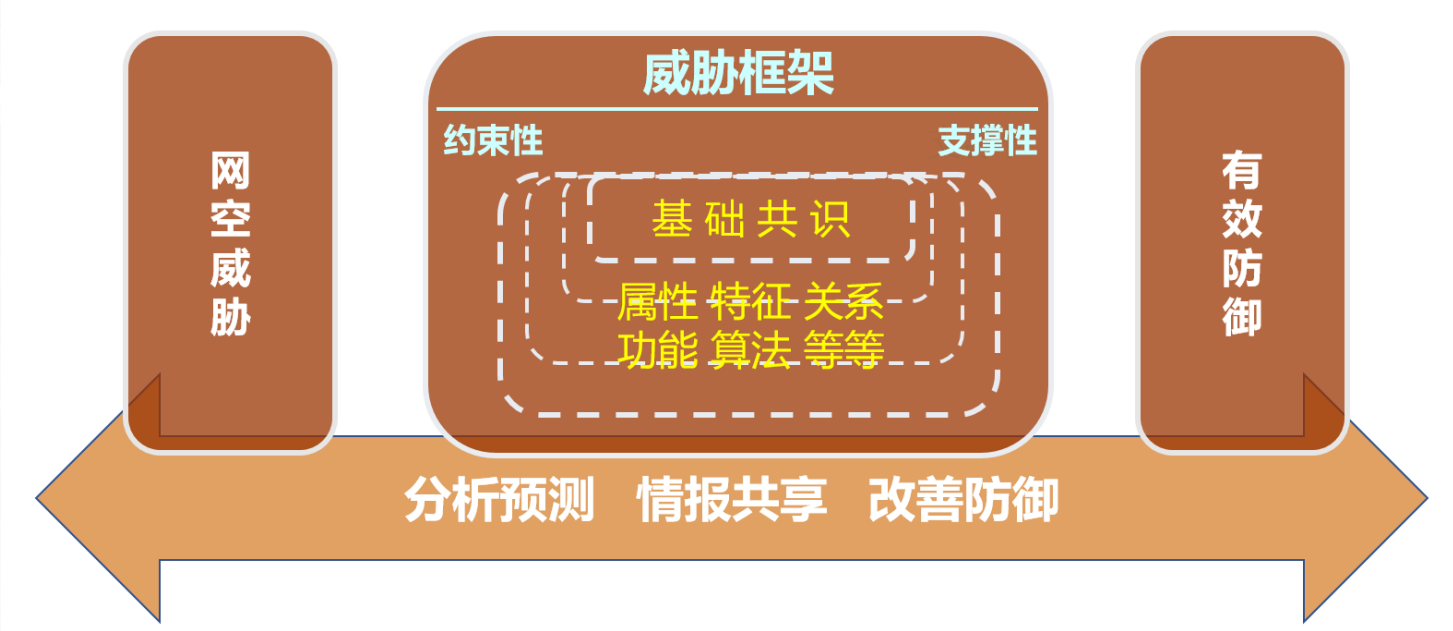
CONTENTS

目 录

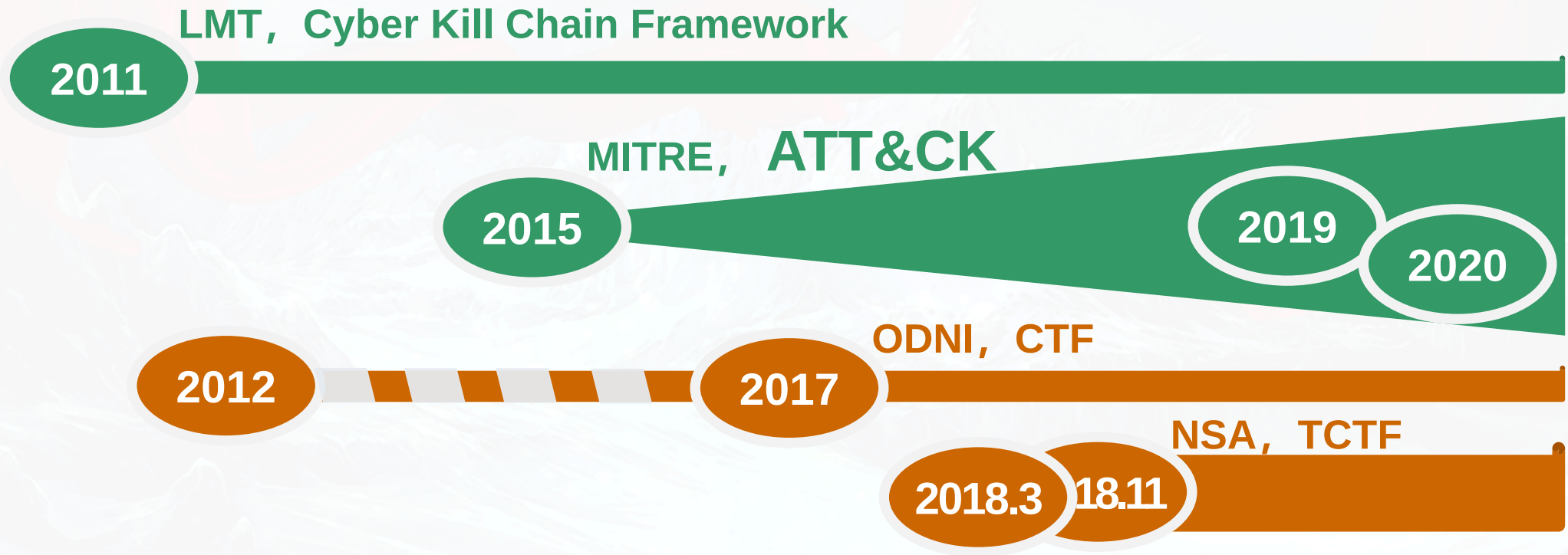
01 网空威胁框架的发展回顾

为什么需要网空威胁框架

- 我们面临日趋多样复杂的网空威胁
- 构建有效的网络防御体系，需要首先形成对威胁的清晰认知
- 威胁框架是系统分析现代复杂威胁的有效手段



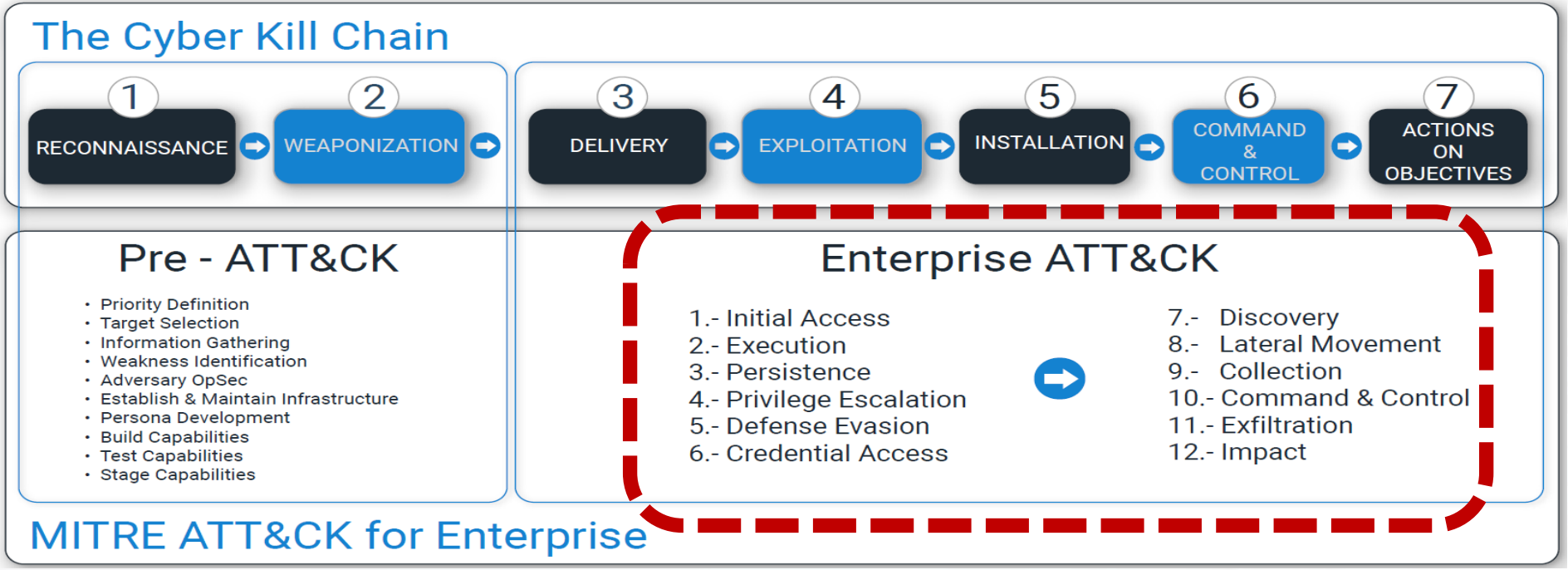
网空威胁框架的构建历程



- **ATT&CK / 对手战术技术公共知识库**
  - Common Knowledge base of Adversary Tactics and Techniques

ATT&CK框架的基本内容

技术域	适用平台
企业域	Windows，Linux，macOS，Cloud，Network
移动域	Android，IOS
工控域	Field Controller/RTU/PLC/IED, Safety Instrumented System/Protection Relay



ATT&CK框架的基本内容

ATT&CK®威胁框架（安天中译版）

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	数据渗出	影响
水坑攻击	利用AppleScript	利用.bash_profile和.bashrc	利用LSASS 驱动程序	操纵访问令牌	操纵访问令牌	安装根证书	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程序	利用CMSTP	利用辅助功能	修改现有服务	借助辅助功能	填充二进制文件	利用InstallUtil	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	操纵账户	Netsh Helper DLL	利用AppCert DLL（注册表项）	利用BITS服务	利用Launchctl	暴力破解	发现浏览器书签	利用COM（组件对象模型）和分布式COM	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加密
添加硬件	利用HTML编译文件	利用AppCert DLL（注册表项）	新建服务	利用AppInit DLL（注册表项）	绕过用户账户控制（UAC）	LC_MAIN劫持	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COM（组件对象模型）和分布式COM	利用AppInit DLL（注册表项）	启动Office应用程序	利用Windows应用程序兼容性框架	清除命令历史	仿冒	获取Web浏览器凭证	发现文件和目录	执行内部鱼叉式钓鱼攻击	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	控制面板项	利用Windows应用程序兼容性框架	路径拦截	绕过用户账户控制（UAC）	利用CMSTP	修改注册表	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	动态数据交换协议（DDE）	利用认证包	修改属性列表	DLL搜索顺序劫持	代码签名	利用Mshta	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钓鱼攻击	通过API执行	利用BITS服务	端口试探	Dylib劫持	投递后编译	删除网络共享连接	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	使用Bootkit	端口监控	提示用户输入合法凭证提权	利用HTML编译文件	利用NTFS交换数据流（ADS）	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	添加浏览器扩展插件	利用PowerShell配置文件	利用事件监控守护进程	利用组件固件	混淆文件或信息	利用Hook	发现周边设备	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	利用Rc.common文件	利用漏洞提权	组件对象模型（COM）劫持	伪造父进程	输入捕捉	发现远程系统	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	重启应用程序	额外窗口内存注入（EWMI）	利用连接代理	修改属性列表	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）劫持	冗余访问	利用文件系统权限漏洞	利用控制面板项	端口试探	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	添加注册表运行键/启动文件夹项	利用Hook	使用DCShadow技术	Process Doppelgänging（仿冒合法进程）	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	利用计划任务	映像劫持	反混淆/解码文件或信息	替换进程内存	LLMNR/NBT-NS投毒和中继	发现安全软件	污染共享内容		端口试探		系统关机/重启
	利用Mshta	Dylib劫持	利用屏幕保护程序	启动守护进程	禁用安全工具	进程注入	网络嗅探	发现软件	利用系统中的第三方软件		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SSP DLL（注册表项）	新建服务	DLL搜索顺序劫持	冗余访问	利用Password Filter DLL	发现					
	利用Regsvcs/Regasm	利用外部远程服务	利用服务器软件组件	伪造父进程	DLL旁路加载	利用Regsvcs/Regasm	收集私钥	发现					
	利用Regsvr32	利用文件系统权限漏洞	利用服务注册表权限漏洞	路径拦截	按条件执行	利用Regsvr32	利用Securityd内存	发现					
	利用Rundll32	隐藏文件和目录	利用Setuid和Setgid位	修改属性列表	利用漏洞规避防御	使用Rootkit	窃取Web会话Cookie	发现					
	利用计划任务	利用Hook	修改快捷方式	端口监控	额外窗口内存注入（EWMI）	利用Rundll32	双因子认证拦截	发					
	使用脚本	利用Hypervisor	会话发起协议（SIP）和受信提供商劫持	利用PowerShell配置文件	修改文件和目录权限	编辑脚本		发					
	利用windows服务	映像劫持	利用启动项	进程注入	删除文件	执行签名的二进制文件代理		虚拟					
	利用签名的二进制文件代理执行	利用内核模块和扩展	利用系统固件	利用计划任务	文件系统逻辑偏移	执行签名的脚本代理							
	利用签名的脚本代理执行	启动代理	利用Systemd服务	利用服务注册表权限漏洞	绕过Gatekeeper	会话发起协议（SIP）和受信提供商劫持							
	利用Source命令	启动守护进程	利用Windows时间服务	利用Setuid和Setgid位	修改组策略	软件加壳							
	加入空格隐藏扩展名	利用Launchctl	利用Trap命令	SID历史注入	隐藏文件目录	加入空格隐藏扩展名							
	利用系统中的第三方软件	添加LC_LOAD_DYLIB	利用有效账户	利用启动项	隐藏用户	模板注入							
	利用Trap命令	利用linux本地任务调度	使用Web Shell	利用Sudo命令	隐藏窗口	修改文件时间戳							
	利用受信的开发工具	利用登录项	利用Windows事件订阅管理器	利用Sudo缓存凭证	HISTCONTROL	利用受信的开发工具							
	诱导用户执行	利用登录脚本	Winlogon Helper DLL	利用有效账户	映像劫持	利用有效账户							
	利用Windows管理规范（WMI）			使用Web Shell	阻止信标捕获	虚拟化/沙箱逃逸							
	利用Windows远程管理服务				删除工具中的信标	利用Web服务							
	利用XSL文件执行脚本				删除主机中的信标	利用XSL文件执行脚本							
					间接执行命令								

技术的细节：

- 定义和描述
- 数据源
- 检测方法
- 现实来源
- 缓解措施
- 等等

ATT&CK Matrix for Enterprise

https://attack.mitre.org/

安天研究院2019年11月译制

安天微信公众号

ATT&CK框架的安全价值

- 以 MITRE ATT&CK 为代表的威胁框架是迄今实用性、实战价值的具佳的高级威胁分析手段

  攻击者视角 + 攻击过程整体分析 + 行为层克制攻击

- 以TTP为分析要素，从现实APT攻击案例中提取TTP，形成知识库

  指导防御方通过 “采集-分析” 来识别攻击行为

- 发展前景良好，且自身积极演进

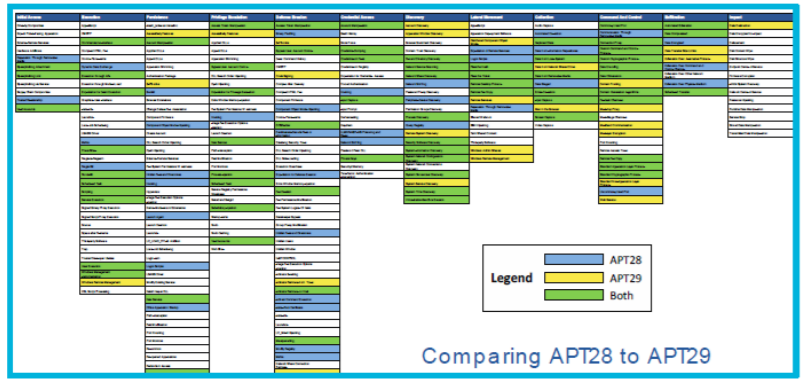
  业已广泛获得安全研究人员与安全厂商的支持

ATT&CK框架的实践运用

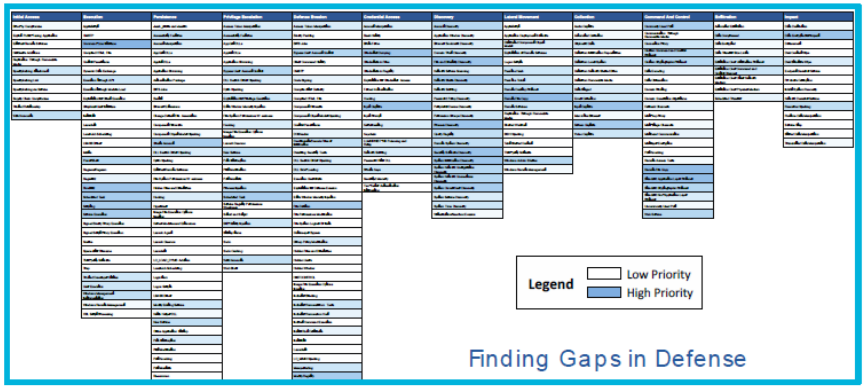
Detection

```
processes = search Process:Create
reg = filter processes where (exe == "reg.exe" and parent_exe
== "cmd.exe")
cmd = filter processes where (exe == "cmd.exe" and
parent_exe != "explorer.exe"")
reg_and_cmd = join (reg, cmd) where (reg.ppid == cmd.pid and
reg.hostname == cmd.hostname)
output reg_and_cmd
```

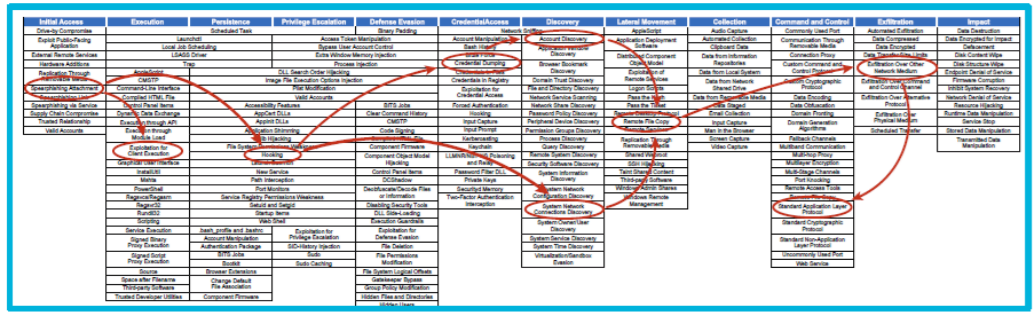
Threat Intelligence



Assessment and Engineering



Adversary Emulation



智者安天下

威胁框架：细粒度对抗

ATT&CK框架的实践运用

安全能力清晰可视
不同环节价值互补

基于端点侧部署的安天智甲终端防御系统的检测和拦截点

基于流量侧部署的安天探海威胁监测系统的可输出的攻击动作标签

智者安天下

02 ATT&CK框架2020年度重要更新

ATT&CK框架版本演化

Version	Start Date	End Date
ATT&CK v8 (current version)	October 27, 2020	n/a
ATT&CK v7	July 8, 2020	October 26, 2020
ATT&CK v7-beta	March 31, 2020	July 7, 2020
ATT&CK v6	October 24, 2019	March 30, 2020
ATT&CK v5	July 31, 2019	October 23, 2019
ATT&CK v4	April 30, 2019	July 30, 2019
ATT&CK v3	October 23, 2018	April 29, 2019

战术扩展

子技术

ATT&CK框架年度重要更新 —— 对手子技术

- 为什么需要 子技术 / Sub-Techniques
  - 有些攻击技术粒度过大，层次欠缺，在现实中无法精确分析，也不利于后期扩展；此外，还有某些技术的类别和名称需要优化调整

    例如 T1193.使用鱼叉式钓鱼附件，粒度比较恰当

    例如 T1064.脚本编程，粒度则过于宽泛

    例如 T1055.进程注入，缺乏层次性

    诸如此类问题，影响了ATT&CK的分析能力、评价能力、扩展能力
  - MITRE 积极响应在实际中遇到的上述问题，推出“子技术版ATT&CK”
- **子技术的意义**
  - **对攻击技术“原子化”**

ATT&CK框架年度重要更新 —— 对手子技术

- 技术向子技术变化的几种情况
  - 情况1：One – to – One

    保留，原样；例如 T1091.通过可移动介质复制

    保留，但所属战术/名称发生了变化；例如 T1105.拷贝远程文件，重命名为 T1105.使用入口工具传输，从归属于 “战术- 横向移动” 改变为归属于 “战术- 命令与控制”

    保留，但降级为子技术；例如 T1097.利用Ticket认证，降级为T1550.使用备用身份验证材料 之下的子技术 T1550.003.利用Ticket认证

  - 直接转换，不需作出相应的处置调整

ATT&CK框架年度重要更新 —— 对手子技术

- 技术向子技术变化的几种情况
  - 情况2：One – to – N

被保留，但自身进行了拆解；
例如，T1003.凭证转储 依然编号为 T1003.操作系统凭证转储（名称微调）
但被拆解为 8 项子技术，如 T1003.001.LSASS进程中凭证转储、
T1003.008./etc/passwd和etc/shadow凭证转储
再例如， T1055.进程注入，分解为11项子技术，如 T1055.001.动态链接库注入、
T1055.002.可执行文件注入

  - 需要作出相应的处置调整

ATT&CK框架年度重要更新 —— 对手子技术

- 技术向子技术变化的几种情况
  - 情况3：One – to – N(n)

例如，T1175.利用COM (组件对象模型)和分布式COM，作为“技术”被废弃；
但同时，其蕴含的动作过程被拆解为 2 个子技术；
分别是 T1559.利用进程间通信 所属子技术 T1559.001.利用组件对象模型(COM)，以及T1021.利用远程服务 所属子技术 T1021.003.利用分布式组件对象模型(DCOM)

  - 需要作出相应的处置调整

ATT&CK框架年度重要更新 —— 对手子技术

Supply Chain Compromise: Compromise Hardware Supply Chain

Other sub-techniques of Supply Chain Compromise (3)

Adversaries may manipulate hardware components in products prior to receipt by a final consumer for the purpose of data or system compromise. By modifying hardware or firmware in the supply chain, adversaries can insert a backdoor into consumer networks that may be difficult to detect and give the adversary a high degree of control over the system. Hardware backdoors may be inserted into various devices, such as servers, workstations, network infrastructure, or peripherals.

ID: T1195.003

Sub-technique of: T1195

Tactic: Initial Access

Platforms: Linux, Windows, macOS

Data Sources: BIOS, Component firmware, Disk forensics, EFI

Version: 1.0

Created: 11 March 2020

Last Modified: 23 March 2020

Version Permalink

Mitigations

Mitigation	Description
Boot Integrity	Use Trusted Platform Module technology and a secure or trusted boot process ... S or EFI to determine if it is vulnerable to modification. [1] [2]

"不含子技术的技术" 以及 "子技术" 才是真正要分析的对手 TTP 中的 "技术/Techniques & 过程/Procedures"

从而也是安全技术/产品/方案 所要覆盖的 能力点

Detection

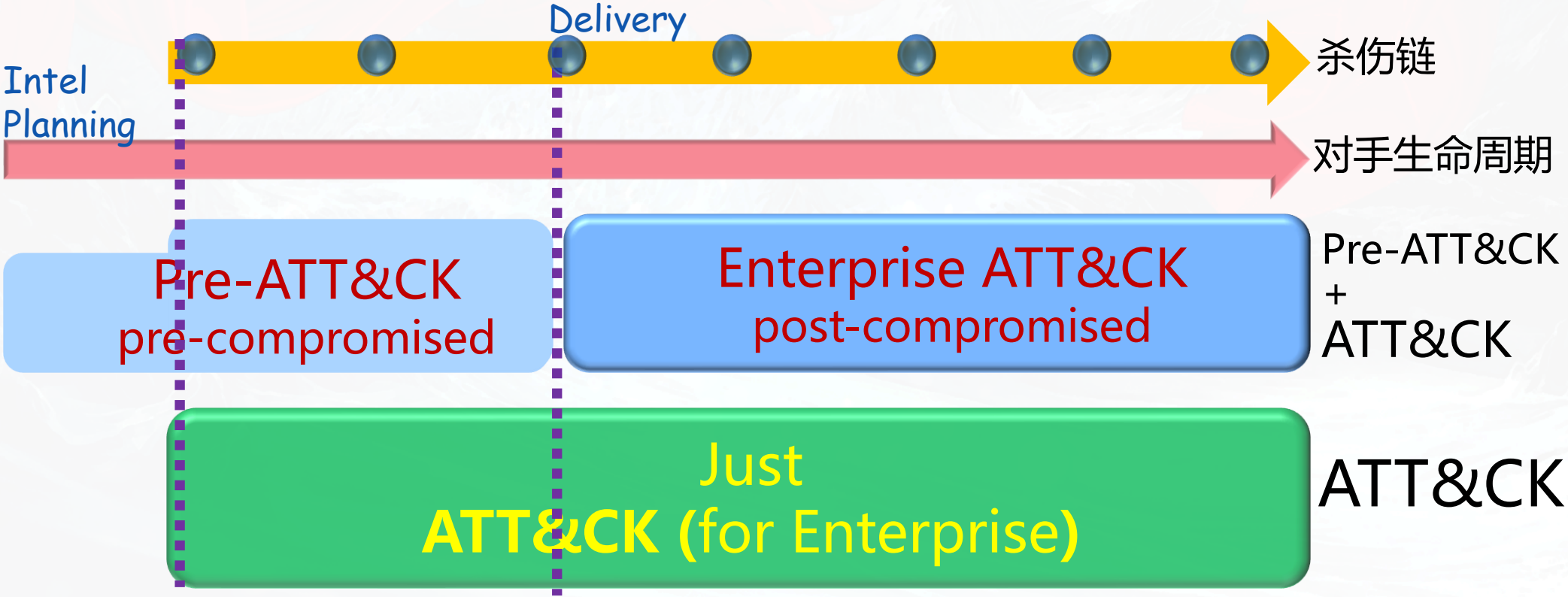
Perform physical inspection of hardware to look for potential tampering. Perform integrity checking on pre-OS boot mechanisms that can be manipulated for malicious purposes.

References

1. Trusted Computing Group. (2008, April 29). Trusted Platform Module (TPM) Summary. Retrieved June 8, 2016.
2. Microsoft. (n.d.). Secure the Windows 10 boot process. Retrieved April 23, 2020.

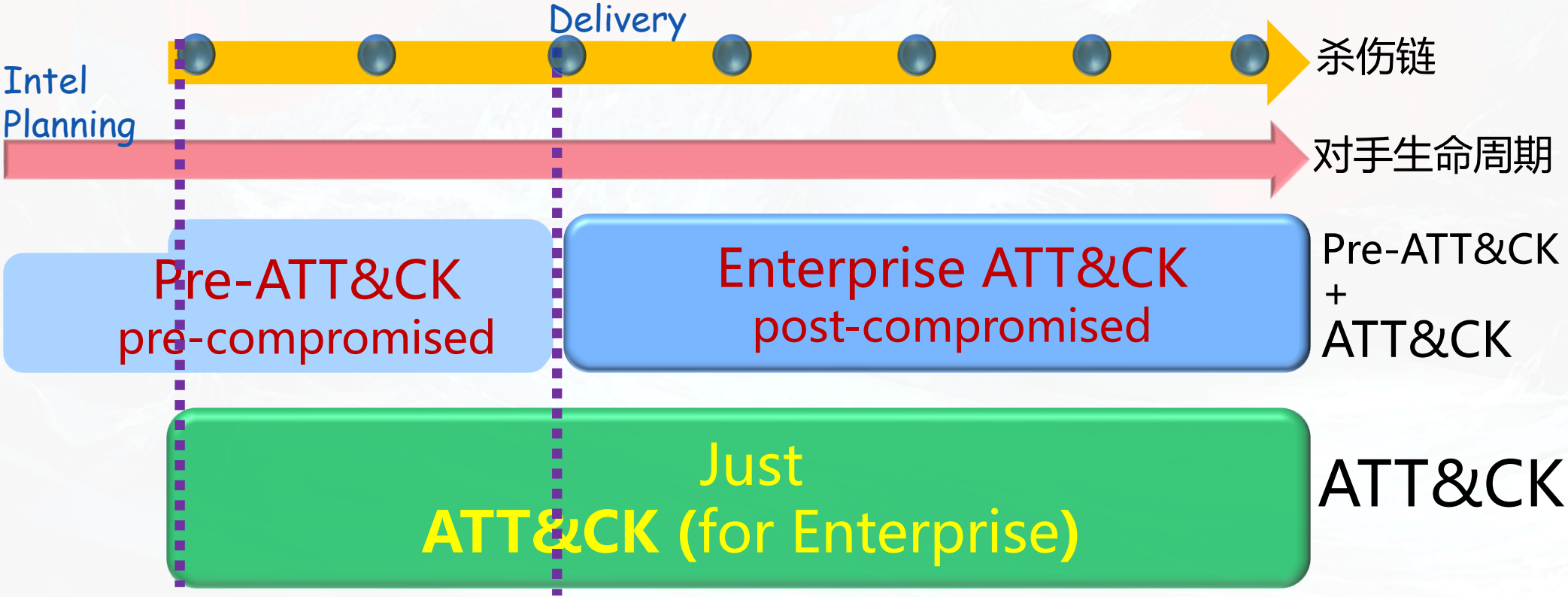
ATT&CK框架年度重要更新 —— 对手战术扩展

- 战术扩展的基本情况



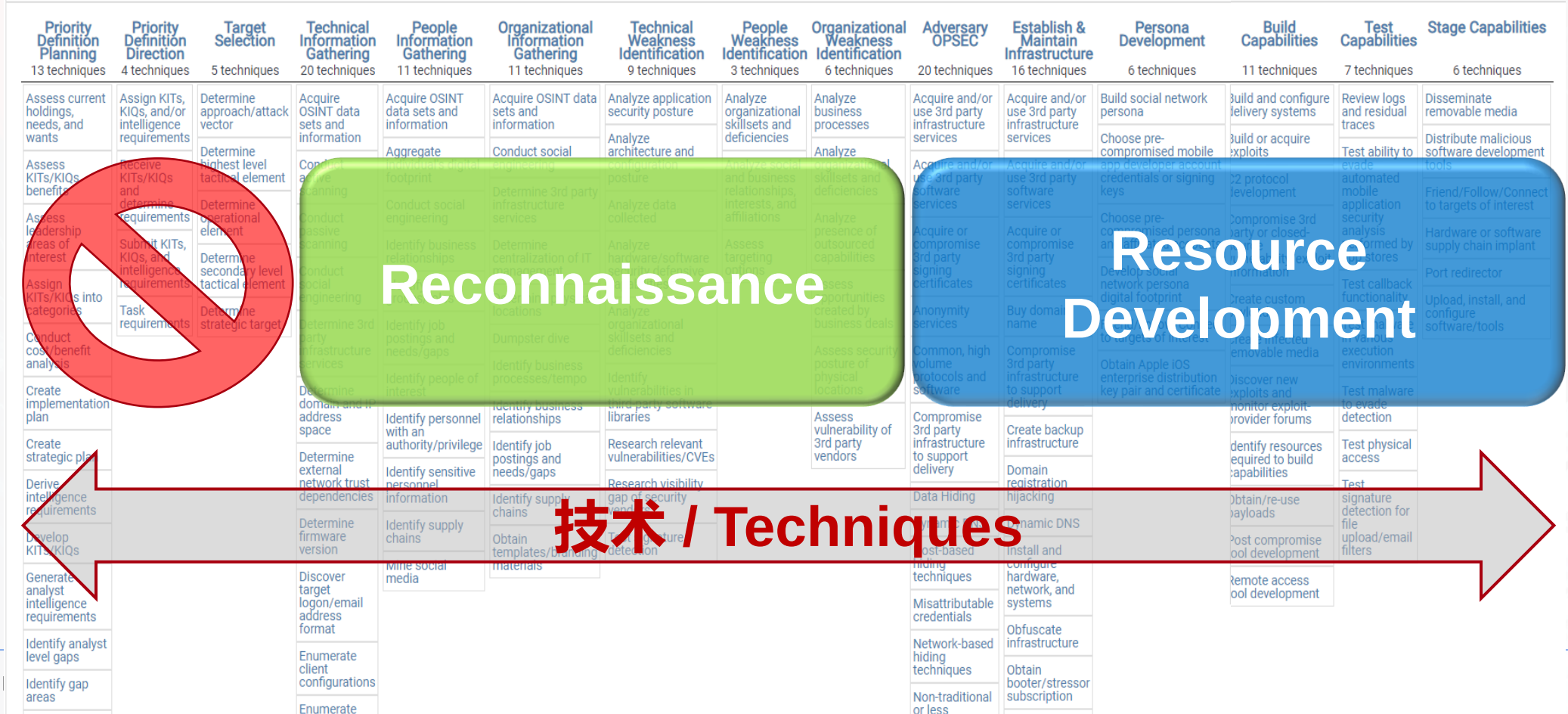
ATT&CK框架年度重要更新 —— 对手战术扩展

- 战术扩展的基本情况



ATT&CK框架年度重要更新 —— 对手战术扩展

- 扩展了哪些战术

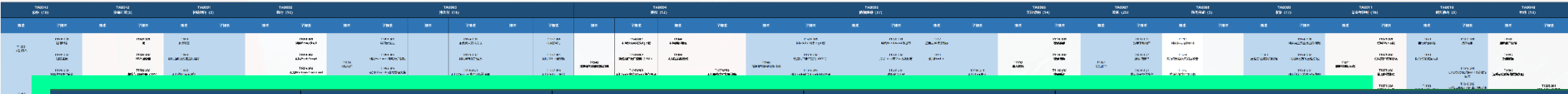


ATT&CK框架年度重要更新 —— 对手战术扩展

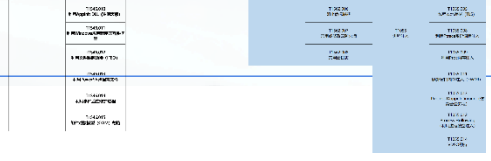
- 战术扩展的意义
  - 将威胁分析从“突破后”扩展到“突破前”，形成对“网空杀伤链”的分析闭环；有效的防御不仅仅要检测“实际已发生的攻击”，更要前摄以识别“潜在的威胁”； 扩展后的威胁框架通过干扰和反制对手的入侵准备，提高对手攻击成本，降低对手攻击效率和成功率，从而更具安全价值
  - 战术扩展后的ATT&CK框架，与NSA-TCTF（NSA，Technical Cyber Threat Framework）框架具有了更好的“对齐性”，更有利于二者的联合分析

ATT&CK框架年度重要更新 —— 对手战术扩展

ATT&CK®威胁框架（安天中译版）



TA0043 侦察（10）		TA0042 资源开发(6)		TA0001 初始访问（9）		TA0002 执行（10）		TA0003 持久化（18）			
技术	子技术	技术	子技术	技术	子技术	技术	子技术	技术	子技术	技术	子技术
T1595 主动扫描	T1595.001 扫描IP段	T1583 获取基础设施	T1583.001 域	T1189 水坑攻击		T1059 利用命令和脚本解释器	T1059.001 利用PowerShell	T1098 操纵账户	T1098.001 添加云凭证		T1546.001 更改默认文件关联
	T1595.002 扫描漏洞		T1583.002 DNS服务器	T1190 利用面向公众的应用程序			T1059.002 利用AppleScript		T1098.002 利用Exchange邮箱账户权限		T1546.002 利用屏幕保护程序
T1592 搜集受害者主机信息	T1592.001 搜集主机硬件信息		T1583.003 虚拟专用服务器（VPS）	T1133 利用外部远程服务			T1059.003 利用Windows Command Shell		T1098.003 添加Office 365全局管理员角色		T1546.003 利用Windows事件订阅管理器
	T1592.002 搜集主机软件信息		T1583.004 服务器	T1200 添加硬件			T1059.004 利用Unix Shell		T1098.004 修改SSH授权秘钥		T1546.004 利用.bash_profile和.bashrc
	T1592.003 搜集主机固件信息		T1583.005 僵尸网络	T1566 网络钓鱼	T1566.001 使用鱼叉式钓鱼附件		T1059.005 利用Visual Basic(VB)	T1197 利用BITS服务			T1546.005 利用Trap命令
	T1592.004 搜集主机客户端配置信息		T1583.006 Web服务		T1566.002 使用鱼叉式钓鱼链接		T1059.006 利用Python		T1547.001 添加注册表运行键/启动文件夹项		T1546.006 添加LC_LOAD_DYLIB
T1589 搜集受害者身份信息	T1589.001 搜集凭证	T1586 入侵账户	T1586.001 社交媒体账户		T1566.003 利用第三方服务进行鱼叉式钓鱼攻击		T1059.007 利用JavaScript/Jscript		T1547.002 利用认证包		T1546.007 Netsh Helper DLL
	T1589.002 搜集电子邮件地址		T1586.002 电子邮件账户	T1091 通过可移动介质复制			T1059.008 利用网络设备的脚本或内置命令解释器（CLI）		T1547.003 利用Windows时间服务	T1546 事件触发执行	T1546.008 利用辅助功能



ATT&CK Matrix for Enterprise

https://attack.mitre.org/

安天研究院2021年01月译制

安天微信公众号

ATT&CK框架年度重要更新 —— 对手战术扩展

Active Scanning: Vulnerability Scanning

Other sub-techniques of Active Scanning (2)

Before compromising a victim, adversaries may scan victims for vulnerabilities that can be used during targeting. Vulnerability scans typically check if the configuration of a target host/application (ex: software and version) potentially aligns with the target of a specific exploit the adversary may seek to use.

These scans may also include more broad attempts to Gather Victim Host Information that can be used to identify more commonly known, exploitable vulnerabilities. Vulnerability scans typically harvest running software and version numbers via server banners, listening ports, or other network artifacts.[1] Information from these scans may reveal opportunities for other forms of reconnaissance (ex: Search Open Websites/Domains or Search Open Technical Databases), establishing operational resources (ex: Develop Capabilities or Obtain Capabilities), and/or initial access (ex: Exploit Public-Facing Application).

ID: T1595.002
Sub-technique of: T1595
Tactic: Reconnaissance
Platforms: PRE
Data Sources: Network device logs, Packet capture
Version: 1.0
Created: 02 October 2020
Last Modified: 24 October 2020

Version Permalink

Mitigations

Mitigation	Description
Pre-compromise	This technique cannot be easily mitigated with preventive controls since it is based on behaviors performed outside of the scope of enterprise defenses and controls. Efforts should focus on minimizing the amount and sensitivity of data available to external parties.

Detection

Monitor for suspicious network traffic that could be indicative of scanning, such as large quantities originating from a single source (especially if the source is known to be associated with an adversary/botnet). Analyzing web metadata may also reveal artifacts that can be attributed to potentially malicious activity, such as referer or user-agent string HTTP/S fields.

Much of this activity may have a very high occurrence and associated false positive rate, as well as potentially taking place outside the visibility of the target organization, making detection difficult for defenders.

Detection efforts may be focused on related stages of the adversary lifecycle, such as during Initial Access.

References

1. OWASP Wiki. (2018, February 16). OAT-014 Vulnerability Scanning. Retrieved October 20, 2020.

威胁框架：细粒度对抗

03 SHIELD积极防御知识库

SHIELD

- 积极防御
- SHIELD知识库内容体系
- 与ATT&CK的关系

积极防御

- 何为积极防御
  - DOD定义：利用受限的进攻性行动和反击，来拒止对手进入一个有争议的地区或位置
  - 网空积极防御：在攻击的具体方法和步骤不为防御者所知的情况下实施主动的、前摄的防御，提升系统在受攻击状态下的生存性和弹性，能够在降低防御成本的同时增加对手的攻击成本
- 积极防御的意义
  - 传统的被动防御技术本质上是静态、被动的，其有效性依赖于对已有网络攻击的先验知识
  - 越来越无法应对日趋复杂且快速变化的网络安全风险，Gartner曾指出，网络防御能力相比于威胁的演进速度而言在持续下降
  - 在这种形势发展背景下，人们对新型防御方案（如积极防御）的需求日益强烈

积极防御

- SHIELD对积极防御的体现
  - 以“通用技术”形成防御基础，以“网空欺骗”和“对手交战”进一步实现积极防御
- SHIELD的价值与不足
  - **是首次系统构建积极防御体系的尝试，为之提供了思路与参考框架**；通过防御方TTP来描述各种防御技术，简化和加速厂商安全能力的建设过程；与ATT&CK形成映射关系，相关防御技术针对性强、且多是基于红蓝对抗演习和实际运维经验提炼出来的，有很好的现实意义和实战作用
  - **尚处于初始阶段**，在当前阶段，对积极防御的支撑主要是高层指引性的（可以视为一个指导框架，但框架的内容有待发展完善），细节有待进一步完善发展（包括分类与结构也可能会有进一步调整）；此外，由于在积极防御空间中有太多可能的活动无法全部列举，因此SHIELD总是不完整的

SHIELD内容体系 —— 技术范畴

- 通用防御技术 / General Cyber Defense
  - 适用于所有防御的基础防御技术；如：日志采集、数据包采集等
- 对手交战 / Adversary Engagement
  - 观察、收集和理解对手针对防御系统的活动
- 网空欺骗 / Cyber Deception
  - 与通用网络防御中的强化和检测活动相比，更为主动、精准，能够捕获到更全面、置信度更高的攻击信息，可以用于检测、威慑或者其他效果
  - **深刻理解网空欺骗的重大价值和发展前景（理念、技术、心理、实践，等）**

故善动敌者，形之，敌必从之；予之，敌必取之。以利动之，以卒（本）待之。

——〔孙子兵法·兵势篇〕

SHIELD内容体系 —— 技术范畴

- 通用防御技术 / General Cyber Defense
  - 适用于所有防御的基础防御技术；如：日志采集、数据包采集等
- 对手交战 / Adversary Engagement
  - 观察、收集和理解对手针对防御系统的活动
- 网空欺骗 / Cyber Deception
  - 与通用网络防御中的强化和检测活动相比，更为主动、精准，能够捕获到更全面、置信度更高的攻击信息，可以用于检测、威慑或者其他效果
  - **深刻理解网空欺骗的重大价值和发展前景（理念、技术、心理、实践，等）**

故善动敌者，形之，敌必从之；予之，敌必取之。以利动之，以卒（本）待之。

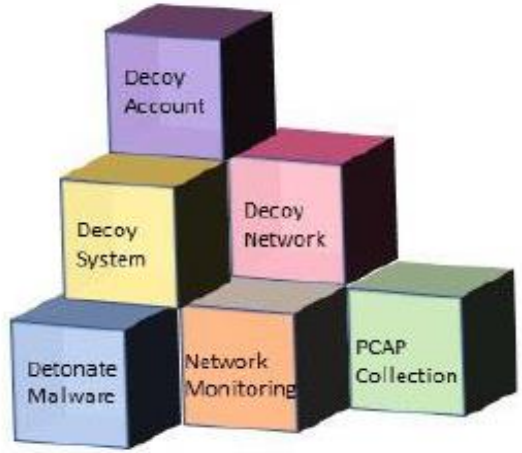
——〔孙子兵法·兵势篇〕

SHIELD内容体系 —— 基本术语

- **战术**（Tactics）：是抽象的防御者目的，即表示防御者试图完成的任务。
- **技术**（ Techniques ）：是防御者可以执行的一般行动，即描述防御如何实现战术。
- **过程**（ Procedures ）：是一个技术的实现（在当前版本中，过程只包含简单的高级别描述，以激发更多思考）。
- **机会空间**（Opportunity Spaces）：描述当攻击者运用他们的技术时引入的高级别积极防御可能性。
- **用例**（Use Cases）：是对防御者如何利用攻击者的行为所呈现的机会的高级别描述；用例有助于进行特定的实现讨论。

SHIELD内容体系 —— 防御模型

- SHIELD积极防御模型主要由技术和战术构成
  - 战术可被比作容器（containers），技术可被比作积木（building blocks）；每个容器（战术）都装着若干积木（技术）；防御者从知识库提供的战术（容器）中，选择最适合积极防御需求的战术；然后防御者可以查看在该战术容器中的技术（积木），并选择允许他们构建最佳积极防御解决方案的技术



SHIELD内容体系 —— 知识库矩阵

MITRE Shield知识库（安天中译版）

DTA0001 引导（18）		DTA0002 收集（18）		DTA0003 约束（11）		DTA0004 检测（20）		DTA0005 干扰（16）		DTA0006 促进（16）		DTA0007 合法化（12）		DTA0008 测试（19）	
技术		技术		技术		技术		技术		技术		技术		技术	
技术中文	技术英文	技术中文	技术英文	技术中文	技术英文	技术中文	技术英文	技术中文	技术英文	技术中文	技术英文	技术中文	技术英文	技术中文	技术英文
DTE0001 管理员权限	Admin Access	DTE0003 API监控	API Monitoring	DTE0001 管理员权限	Admin Access	DTE0003 API监控	API Monitoring	DTE0001 管理员权限	Admin Access	DTE0001 管理员权限	Admin Access	DTE0004 应用多样性	Application Diversity	DTE0001 管理员权限	Admin Access
DTE0003 API监控	API Monitoring	DTE0004 应用多样性	Application Diversity	DTE0006 基线建立	Baseline	DTE0004 应用多样性	Application Diversity	DTE0004 应用多样性	Application Diversity	DTE0004 应用多样性	Application Diversity	DTE0008 痕迹仿真	Burn-In	DTE0003 API监控	API Monitoring
DTE0004 应用多样性	Application Diversity	DTE0005 备份与恢复	Backup and Recovery	DTE0010 诱饵账户	Decoy Account	DTE0007 行为分析	Behavioral Analytics	DTE0005 备份与恢复	Backup and Recovery	DTE0007 行为分析	Behavioral Analytics	DTE0010 诱饵账户	Decoy Account	DTE0004 应用多样性	Application Diversity
DTE0010 诱饵账户	Decoy Account	DTE0010 诱饵账户	Decoy Account	DTE0014 诱饵网络	Decoy Network	DTE0010 诱饵账户	Decoy Account	DTE0006 基线建立	Baseline	DTE0008 痕迹仿真	Burn-In	DTE0011 诱饵内容	Decoy Content	DTE0005 备份与恢复	Backup and Recovery
DTE0011 诱饵内容	Decoy Content	DTE0011 诱饵内容	Decoy Content	DTE0018 受控环境执行	Detonate Malware	DTE0011 诱饵内容	Decoy Content	DTE0007 行为分析	Behavioral Analytics	DTE0010 诱饵账户	Decoy Account	DTE0012 诱饵凭证	Decoy Credentials	DTE0010 诱饵账户	Decoy Account
DTE0012 诱饵凭证	Decoy Credentials	DTE0012 诱饵凭证	Decoy Credentials	DTE0020 硬件操控	Hardware Manipulation	DTE0012 诱饵凭证	Decoy Credentials	DTE0011 诱饵内容	Decoy Content	DTE0011 诱饵内容	Decoy Content	DTE0013 诱饵多样性	Decoy Diversity	DTE0011 诱饵内容	Decoy Content
DTE0014 诱饵网络	Decoy Network	DTE0014 诱饵网络	Decoy Network	DTE0022 隔离	Isolation	DTE0014 诱饵网络	Decoy Network	DTE0012 诱饵凭证	Decoy Credentials	DTE0012 诱饵凭证	Decoy Credentials	DTE0014 诱饵网络	Decoy Network	DTE0012 诱饵凭证	Decoy Credentials
DTE0015 诱饵角色信息	Decoy Persona	DTE0017 诱饵系统	Decoy System	DTE0023 迁移攻击向量	Migrate Attack Vector	DTE0017 诱饵系统	Decoy System	DTE0014 诱饵网络	Decoy Network	DTE0013 诱饵多样性	Decoy Diversity	DTE0015 诱饵角色信息	Decoy Persona	DTE0013 诱饵多样性	Decoy Diversity
DTE0016 诱饵进程	Decoy Process	DTE0018 受控环境执行	Detonate Malware	DTE0026 网络操控	Network Manipulation	DTE0019 电子邮件操控	Email Manipulation	DTE0019 电子邮件操控	Email Manipulation	DTE0015 诱饵角色信息	Decoy Persona	DTE0016 诱饵进程	Decoy Process	DTE0014 诱饵网络	Decoy Network
DTE0017 诱饵系统	Decoy System	DTE0019 电子邮件操控	Email Manipulation	DTE0032 安全控制	Security Controls	DTE0021 狩猎	Hunting	DTE0020 硬件操控	Hardware Manipulation	DTE0017 诱饵系统	Decoy System	DTE0017 诱饵系统	Decoy System	DTE0015 诱饵角色信息	Decoy Persona
DTE0018 受控环境执行	Detonate Malware	DTE0025 网络多样性	Network Diversity	DTE0036 软件操控	Software Manipulation	DTE0022 隔离	Isolation	DTE0022 隔离	Isolation	DTE0025 网络多样性	Network Diversity	DTE0025 网络多样性	Network Diversity	DTE0017 诱饵系统	Decoy System
DTE0023 迁移攻击向量	Migrate Attack Vector	DTE0027 网络监控	Network Monitoring			DTE0026 网络操控	Network Manipulation	DTE0026 网络操控	Network Manipulation	DTE0026 网络操控	Network Manipulation	DTE0030 仿真数据	Pocket Litter	DTE0018 受控环境执行	Detonate Malware
DTE0025 网络多样性	Network Diversity	DTE0028 PCAP收集	PCAP Collection			DTE0027 网络监控	Network Monitoring	DTE0032 安全控制	Security Controls	DTE0029 外设管理	Peripheral Management			DTE0023 迁移攻击向量	Migrate Attack Vector
DTE0026 网络操控	Network Manipulation	DTE0029 外设管理	Peripheral Management			DTE0028 PCAP收集	PCAP Collection	DTE0033 标准操控流程	Standard Operating Procedure	DTE0030 仿真数据	Pocket Litter			DTE0025 网络多样性	Network Diversity

SHIELD内容体系 —— 知识库矩阵

Decoy Account

Create an account that is used for active defense purposes.

A decoy account is one that is created specifically for defensive or deceptive purposes. It can be in the form of user accounts, service accounts, software accounts, etc. The decoy account can be used to make a system, service, or software look more realistic or to entice an action.

Details

ID: DTE0010

Tactics: Legitimize, Channel, Collect, Detect, Facilitate, Contain, Tes

Opportunities

ID	Description
DOS0001	There is an opportunity to study the adversary and collect first-hand observations about them and their tools.
DOS0004	There is an opportunity to introduce user accounts that are used to make a system look more realistic.
DOS0187	In an adversary engagement operation, there is an opportunity to present decoy accounts to the adversary during the enumeration process.
DOS0253	There is an opportunity to introduce decoy information, users, systems, etc. to influence an adversary's future actions.

Use Cases

ID	Description
DUC0004	A defender can create decoy user accounts which are used to make a decoy system or network look more realistic.
DUC0044	A defender can use decoy accounts and monitor them for any activity that might reveal adversary manipulation.
DUC0187	During an adversary engagement operation, a defender can utilize decoy accounts to provide content to an adversary and encourage additional activity.

Procedures

ID	Description
DPR0020	Create a user account with a specified job function. Populate the user account's groups, description, logon hours, etc., with decoy data that looks normal in the environment.
DPR0021	Create a user that has a valid email account. Use this account in such a way that the email address could be harvested by the adversary. This can be monitored to see if it is used in future attacks.

SHIELD与ATT&CK的关系

- 映射带来更全面的防御价值
  - 二者联合运用，发挥更全面的安全价值
  - 在ATT&CK中发现的对手行动，经常能为防御者提供反制的机会；MITRE把SHIELD的技术映射到ATT&CK上，使其能够制定计划以利用这些机会为防御者创造优势；通过将ATT&CK和SHIELD一起使用可以帮助防御者加深对对手行为和交战的理解，并提出防御者可以发起更积极防御的方式

SHIELD与ATT&CK的关系

Decoy Account

Create an account that is used for active defense purposes.

A decoy account is one that is created specifically for defensive or deceptive purposes. It can be in the form of user accounts, service accounts, software accounts, etc. The decoy account can be used to make a system, service, or software look more realistic or to entice an action.

Details

ID: DTE0010

Tactics: Legitimize, Channel, Colle
Test

ATT&CK® Techniques

ID	Name	ATT&CK Tactics
T1078	Valid Accounts	Defense Evasion, Persistence, Privilege Escalation, Initial Access
T1087	Account Discovery	Discovery
T1098	Account Manipulation	Persistence
T1589	Gather Victim Identity Information	Reconnaissance
T1598	Phishing for Information	Reconnaissance

SHIELD与ATT&CK的关系

Mapping To APT28

APT28 is a threat group that has been attributed to Russia's General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS) military unit 26165. This group has been active since at least 2004. APT28 reportedly compromised the Hillary Clinton campaign, the Democratic National Committee, and the Democratic Congressional Campaign Committee in 2016 in an attempt to interfere with the U.S. presidential election. In 2018, the US indicted five GRU Unit 26165 officers associated with APT28 for cyber operations (including close-access operations) conducted between 2014 and 2018 against the World Anti-Doping Agency (WADA), the US Anti-Doping Agency, a US nuclear facility, the Organization for the Prohibition of Chemical Weapons (OPCW), the Spiez Swiss Chemicals Laboratory, and other organizations. Some of these were conducted with the assistance of GRU Unit 74455, which is also referred to as Sandworm Team.

Details

ATT&CK ID: G0007

Associated Groups:
APT28, SNAKEMACKEREL, Swallowtail, Group 74, Sednit, Sofacy, Pawn Storm, Fancy Bear, STRONTIUM, Tsar Team, Threat Group-4127, TG-4127

Note: This page uses Adversary Group data from MITRE ATT&CK.

Disclaimer: We present this mapping to stimulate thinking about active defense options to combat this adversary, not to present all possibilities. We invite you to use this as a guide and add your own use cases for applying Shield techniques to counter each adversary action.

Note: All ATT&CK Group sub-technique mappings have been remapped to their parent technique and were derived from Group Technique mappings in ATT&CK v8.

ATT&CK Technique	Opportunity Space	AD Technique	Use Case
T1001 - Data Obfuscation	There is an opportunity to detect adversary activity that uses obfuscated communication.	DTE0028 - PCAP Collection	A defender can capture network traffic for a compromised system and look for abnormal network traffic that may signal data obfuscation.
T1001 - Data Obfuscation	There is an opportunity to reveal data that the adversary has tried to protect from defenders	DTE0031 - Protocol Decoder	Defenders can develop protocol decoders that can decrypt network capture data and expose an adversary's command and control traffic as well as their exfiltration activity.
T1003 - OS Credential Dumping	There is an opportunity to deploy a tripwire that triggers an alert when an adversary touches a network resource or uses a specific technique.	DTE0012 - Decoy Credentials	A defender can seed systems with decoy credentials in a variety of locations and establish alerting that will trigger if an adversary harvests the credentials and attempts to use them.
T1005 - Data from Local System	In an adversary engagement scenario, there is an opportunity to add legitimacy by ensuring the local system is with fully populated with content.	DTE0030 - Pocket Litter	A defender can stage a variety of pocket litter files to bolster the legitimacy of the local system.

SHIELD与ATT&CK的关系

ATT&CK Mapping by Tactic

ATT&CK Tactic	Description
TA0043 - Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
TA0042 - Resource Development	The adversary is trying to establish resources they can use to support operations.
TA0001 - Initial Access	The adversary is trying to get into your network.
TA0002 - Execution	The adversary is trying to run malicious code.
TA0003 - Persistence	The adversary is trying to maintain their foothold.
TA0004 - Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005 - Defense Evasion	The adversary is trying to avoid being detected.
TA0006 - Credential Access	The adversary is trying to steal account names and passwords.
TA0007 - Discovery	The adversary is trying to figure out your environment.
TA0008 - Lateral Movement	The adversary is trying to move through your environment.
TA0009 - Collection	The adversary is trying to gather data of interest to their goal.
TA0010 - Exfiltration	The adversary is trying to steal data.
TA0011 - Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0040 - Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

SHIELD与ATT&CK的关系

Complete ATT&CK® Mapping

The table below shows the mapping of ATT&CK® Techniques from all ATT&CK® Tactics to Active Defense Opportunities, Techniques, and Use Cases.

ATT&CK Technique	Opportunity Space	AD Technique	Use Case
T1001 - Data Obfuscation	There is an opportunity to detect adversary activity that uses obfuscated communication.	DTE0028 - PCAP Collection	A defender can capture network traffic for a compromised system and look for abnormal network traffic that may signal data obfuscation.
T1001 - Data Obfuscation	There is an opportunity to reveal data that the adversary has tried to protect from defenders	DTE0031 - Protocol Decoder	Defenders can develop protocol decoders that can decrypt network capture data and expose an adversary's command and control traffic as wel as their exfiltration activity.
T1003 - OS Credential Dumping	There is an opportunity to deploy a tripwire that triggers an alert when an adversary touches a network resource or uses a specific technique.	DTE0012 - Decoy Credentials	A defender can seed systems with decoy credentials in a variety of locations and establish alerting that will trigger if an adversary harvests the credentials and attempts to use them.
T1005 - Data from Local System	n an adversary engagement scenario, there is an opportunity to add egitimacy by ensuring the local system is with fully populated with content.	DTE0030 - Pocket Litter	A defender can stage a variety of pocket litter files to bolster the legitimacy of the local system.
T1005 - Data from Local System		DTE0030 - Pocket Litter	
T1006 - Direct Volume Access		DTE0036 - Software Manipulation	how that API call functions.
T1007 - System Service Discovery	There is an opportunity for the defender to observe the adversary and control what they can see, what effects they can have, and/or what data they can access.	DTE0003 - API Monitoring	A defender can monitor and analyze operating system functions calls for detection and alerting.
T1007 - System Service Discovery	There is an opportunity for the defender to observe the adversary and control what they can see, what effects they can have, and/or what data they can access.	DTE0036 - Software Manipulation	A defender could manipulate the command to display services an adversary would expect to see on a system, or to shown them unexpected services.

在对手交战场景中，有机会提供各种主题的内容，以了解敌方似乎感兴趣的信息类型

防御者可放置各种垃圾文件，以确定对手是否对特定的文件类型、主题等感兴趣

SHIELD与ATT&CK的关系

- 更多融合运用

例如，通过ATT&CK优化SHIELD网空欺骗

使用攻击技术 “T1217 发现浏览器书签”，意味着

- 对手期望浏览器
- 对手希望浏览器有书签
- 对手期望一个交互式用户

Turla
使用攻击技术“T1049 发现系统网络连接”

- 暴露“虚假”：创建到目标主机的连接
- 隐蔽“真实”：隐藏登录系统的连接

SHIELD小结

- MITRE SHIELD 首次对系统构建积极防御体系给出了理论指导和参考框架 ； 防御者能够利用SHIELD中包含的战术和技术，来更好地创建、使用、操作积极防御解决方案
- 从ATT&CK演进到SHIELD是自然的过程，SHIELD在防御侧与ATT&CK保持一致；并且，通过对ATT&CK攻击技战术的有效利用，能够最大化防御能力
- SHIELD处在发展阶段中，未来通过结构与内容的改进完善，能够适应更加复杂的积极防御要求

谢谢大家