ATT&CK 在攻击事件关联分析中的实践

2021 年 9 月

目录

提出 ATT&CK 的背景

2011年，洛马提出杀伤链（Kill Chain）将网络攻击过程模型化，定义了攻击者攻击要完成的七个阶段。但杀伤链的描述粒度仍然较粗、缺乏相应的细节也并未形成统一描述不便共享使用。

2013 年，MITRE 在 Kill Chain 的基础上，意图构建一套从攻击者视角出发、比 Kill Chain 粒度更细、有实际技术细节支撑的知识模型，在内部整合研发了 ATT&CK 框架的雏形，后公开对外发布。

ATT&CK 的基本内容

MITRE ATT&CK 是一个基于实际观察到的攻击技战术构建的知识库，可用于政府、企业和网络安全产品中开发特定的威胁模型和方法。

ATT&CK 的核心概念包括：矩阵（Matrices）、战术（Tactics）、技术（Techniques）、缓解措施（Mitigations）、攻击组织（Groups）、攻击工具（Software）。

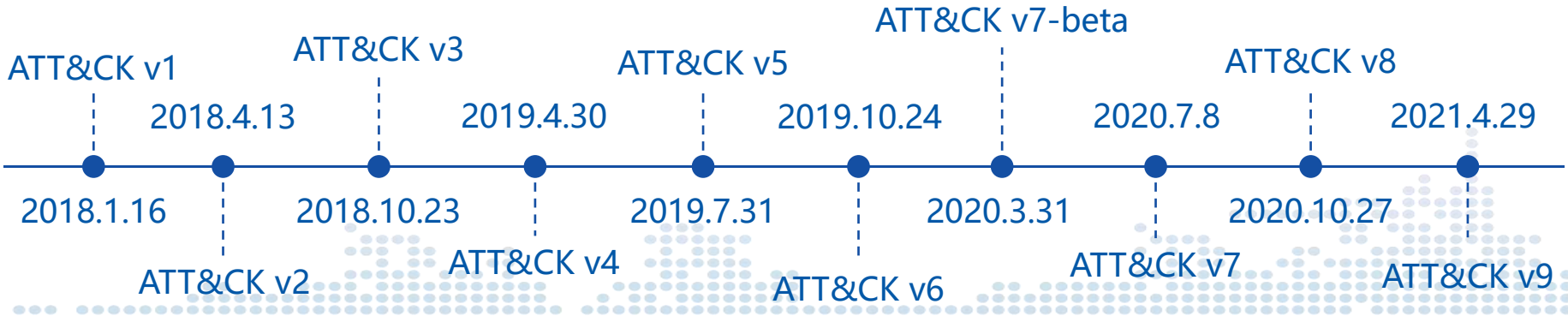
矩阵	战术阶段	技术项	缓解措施
Enterprise	14	185	42
ICS	12	81	
Mobile	14	89	12

	部分示例
攻击组织	APT 28、APT 29、APT 32、Lazarus、Sidewinder、TA505、Turla、 等
攻击工具	CobaltStrike、Denis、Empire、Flame、gh0st RAT、Mimikatz、NotPetya 等

根据公开披露的分析报告，ATT&CK 提供了 122 个攻击组织、585 个攻击工具的相关技战术信息。

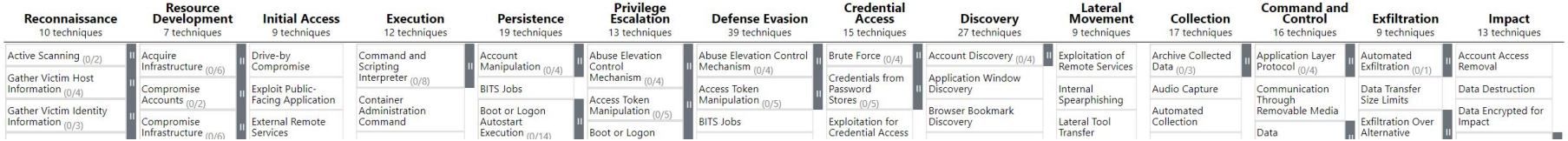
ATT&CK 威胁框架演进

- 2013 年，MITRE 在内部研究提出了 ATT&CK 框架。2014 年只包含 64 个技术项，2015 年 5 月正式对外发布。随后 MITRE 不断对其进行更新，在 2016 年已经包含 121 个技术项。
- 2017 年，ATT&CK 扩展覆盖全平台（Windows、Mac 与 Linux）。2018 年开始按照正式版本控制管理框架开发，开启 ATT&CK 1.0 时代。2019 年，扩展覆盖云平台（ATT&CK for Cloud），同时 Enterprise ATT&CK 技术项达到 266 个。
- 2020 年将 PRE-ATT&CK 并入 Enterprise ATT&CK 中，并且拆分\合并形成了 348 个子技术项，技术项降到 177 个。同年，工控领域的威胁矩阵（ATT&CK for ICS）发布。
- 2021 年，Enterprise ATT&CK 扩展覆盖容器（ATT&CK for Containers）。到目前为止，核心的 Enterprise ATT&CK 包含 185 个技术项和 367 个子技术项。



Enterprise ATT&CK 概览

最新版本的 Enterprise ATT&CK 框架共计包含 14 个战术阶段（前期侦察、资源开发、初始访问、执行、持久化、权限提升、防御逃避、凭据访问、探测发现、横向移动、信息收集、命令控制、外带渗漏、影响）、185 个技术项和 367 个子技术项。涵盖 PRE、Windows、macOS、Linux、Cloud、Network、Containers 共计七个不同视角下的子矩阵。



每个技术项主要包含技术项 ID、子技术项 ID、归属战术阶段、覆盖平台、数据来源、缓解措施、检测建议等信息。以 T1087 技术项（账户发现）为例，如下所示。

Mitigations

ID	Mitigation	Description
M1028	Operating System Configuration	Prevent administrator accounts from being enumerated when an application is elevating through UAC since it can lead to the disclosure of account names. The Registry key is located `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\CredUI\EnumerateAdministrators`. It can be disabled through GPO: Computer Configuration > [Policies] > Administrative Templates > Windows Components > Credential User Interface: E numerate administrator accounts on elevation. [3]

Detection

System and network discovery techniques normally occur throughout an operation as an adversary learns the environment. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as Lateral Movement, based on the information obtained.

Monitor processes and command-line arguments for actions that could be taken to gather system and network information. Remote access tools with built-in features may interact directly with the Windows API to gather information. Information may also be acquired through Windows system management tools such as Windows Management Instrumentation and PowerShell.

Monitor for processes that can be used to enumerate user accounts, such as `net.exe` and `net1.exe`, especially when executed in quick succession.[4]

ID: T1087

Sub-techniques: T1087.001, T1087.002, T1087.003, T1087.004

ⓘ Tactic: Discovery

ⓘ Platforms: Azure AD, Google Workspace, IaaS, Linux, Office 365, SaaS, Windows, macOS

ⓘ Permissions Required: User

ⓘ Data Sources: Command: Command Execution, File: File Access, Process: Process Creation, User Account: User Account Metadata

ⓘ CAPEC ID: CAPEC-575

Contributors: Daniel Stepanic, Elastic; Microsoft Threat Intelligence Center (MSTIC); Travis Smith, Tripwire

Version: 2.3

Created: 31 May 2017

Last Modified: 14 April 2021

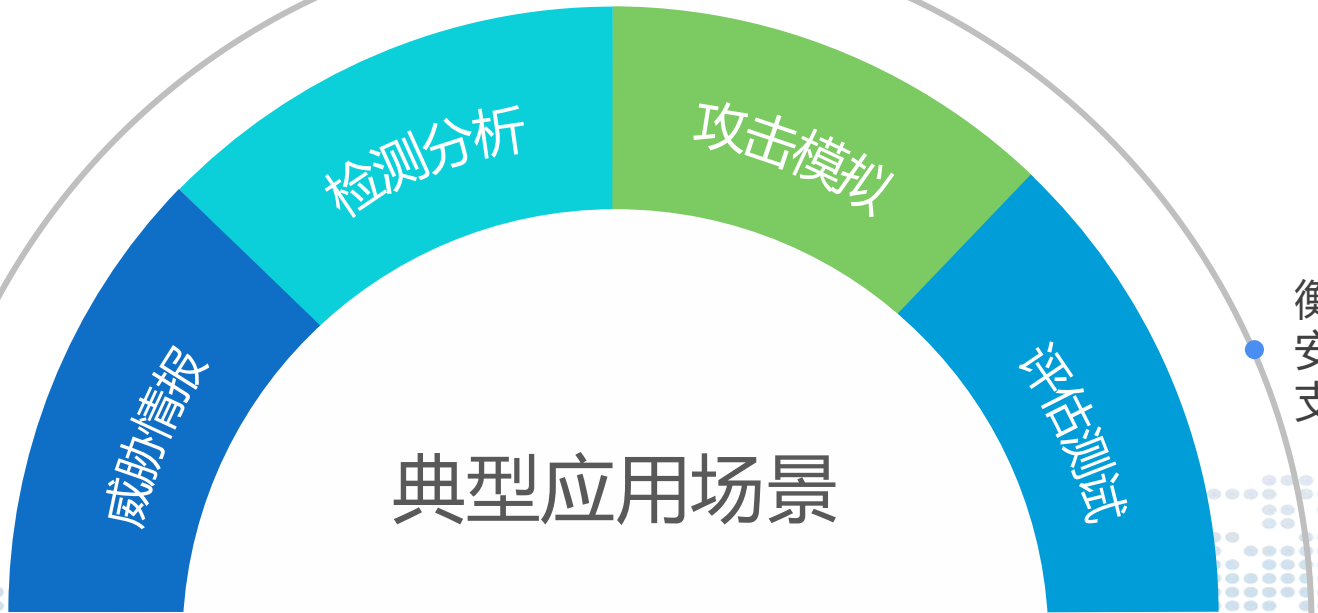
ATT&CK 框架典型应用场景

帮助网络防御人员
开发并持续改进能够
检测攻击行为的技术手段

提供一种通用框架
红队可用于模拟特定攻击
技战术并整体规划攻击行动

为安全分析人员
提供通用语言
处理威胁情报

衡量评估组织
安全能力并
支撑最终决策



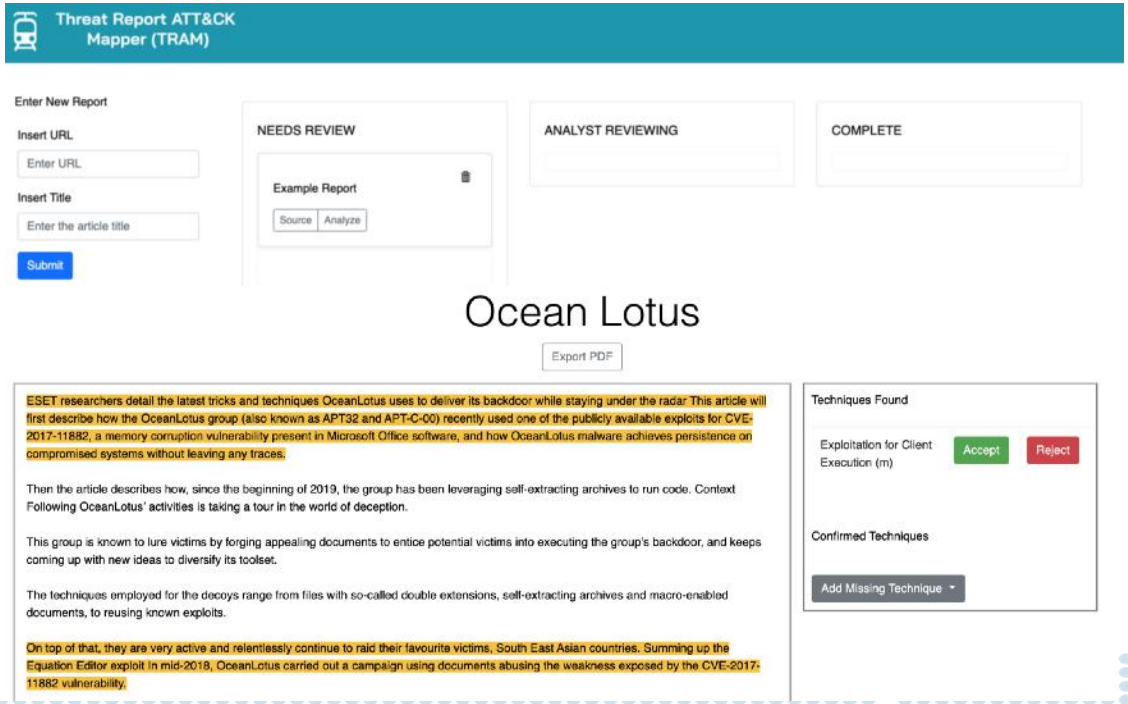
ATT&CK 框架典型应用场景：威胁情报

情报交换

ATT&CK 规范化的威胁情报可以在组织间更好地进行情报的交换与沟通，帮助分析人员更好地理解攻击者的行为。ATT&CK 也可以与网络威胁情报领域中的其他框架/标准，如结构化威胁信息表达式（STIX）、通用攻击模式枚举与分类（CAPEC）等结合使用。

情报生产

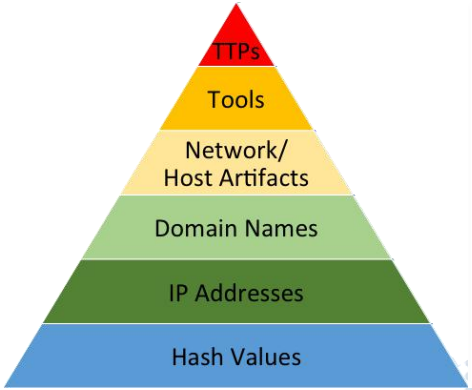
MITRE 开发了开源威胁情报提取工具 TRAM，用于自动从英文的分析报告中解析文件内容中存在的攻击行为，映射到对应的 ATT&CK 技术项。

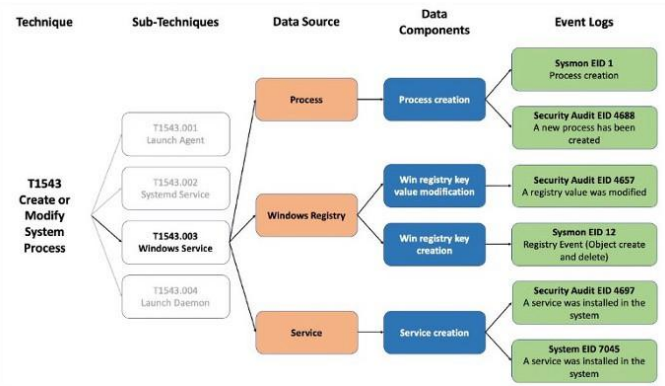


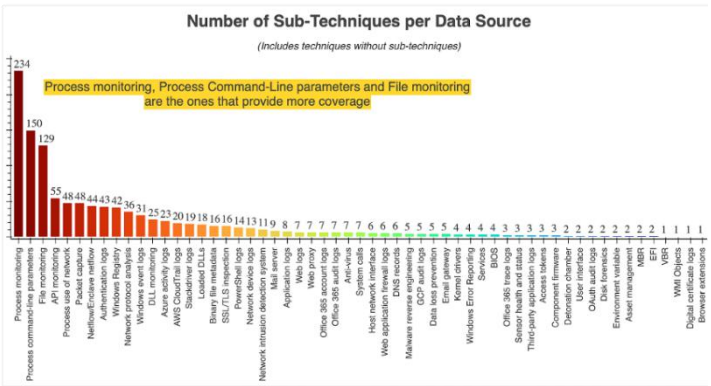
ATT&CK 框架典型应用场景：检测分析

ATT&CK 框架为检测能力的覆盖提供了衡量标准，可以利用 ATT&CK 针对性地弥合威胁检测能力和面临风险之间的差距。提升安全检测分析能力由低层的 IOC 类威胁指标向高层的 TTP 类覆盖。安全厂商也可以利用 ATT&CK 指导检测类产品的研发，跟踪改善检测能力。

新版本的 ATT&CK 框架中更加强调数据来源（Data Source）的重要性并予以重构，更加详细地指出为了检测技术项/子技术应该通过什么技术、收集什么数据







ATT&CK 框架典型应用场景：攻击模拟

ATT&CK 可以应用在攻击模拟（Adversary Emulation）场景中，通过模拟真实攻击者的攻击行为进行安全测试。由于攻击者会持续改进攻击技战术（TTP），已有的安全检测或安全控制措施可能面临失效的风险，或者攻击者可能已经潜伏了很长时间却未被发现。攻击模拟可以有目的性的测试安全检测或者应急响应的有效性，以 ATT&CK 框架的视角来衡量网络安全成熟度。

业界常见的攻击模拟工具如下所示：

项目名称	开发者	覆盖	Agent	是否更新
Atomic Red Team	Red Cannary	最多	无	十分活跃
CALDERA	MITRE	较多	有（Sandcat）	十分活跃
Purple Team Automation	Praetorian	较多	无	较为活跃
Red Team Automation	ENDGAME	较少	无	很不活跃

ATT&CK 框架典型应用场景：评估测试

MITRE 每年模拟不同的攻击组织对参加评估的厂商进行检测能力测试，评估测试不打分、不排名，检测结果对所有人开放。评估测试吸引了数十家厂商参与其中，包括微软、思科等大厂；ESET、卡巴斯基、Bitdefender、赛门铁克等老牌杀软厂商；CrowdStrike、Cylance、Carbon Black 等 EDR 厂商以及 FireEye、Palo Alto Network 等专业安全公司。

评估测试迄今为止已经完成了三轮，2021 年的评估测试同时提供了 Enterprise 与 工控（ICS）两个威胁场景

时间	模拟组织	厂商数量	简要描述
2018	APT 3	12	模拟 APT 3 使用不同工具进行提权/横向移动/窃取数据
2019	APT 29	21	模拟 APT 29“窃取数据”和“窃取并破坏”的两个场景
2020	Carbanak 与 FIN 7	29	覆盖 Windows 与 Linux 的复杂恶意软件场景
2021	Wizard Spider 与 Sandworm	-	聚焦于数据加密的影响，如勒索软件和专门破坏的恶意软件
	TRITON	-	模拟能源行业的燃烧管理系统被攻击

目录

ATT&CK 在攻击事件关联分析中的实践

01

网空威胁映射

1、将恶意样本特征和网络事件准确映射到 ATT&CK 网空威胁框架攻击矩阵

2、标签体系支持可视化展示；具备统一性和可扩展性

02

多源数据运营

1、基于多种类、多来源数据构建面向实体、关系、属性的关联分析知识数据

2、依托提取生成的实体关系数据支撑多个类型的业务场景使用，进行快速关联拓线

03

攻击场景还原

1、利用多源数据，快速、全面、准确的在全网定位失陷影响范围

2、对攻击事件的攻击过程进行还原挖掘

04

组织威胁狩猎

1、从技战术角度深入刻画攻击组织的攻击手段与攻击能力

2、通过攻击组织常用的技战术手段可以形成针对性的威胁狩猎能力

网空威胁映射 - ATT&CK 技术项标定

依据攻击技术特征构建 ATT&CK 技术项映射规则，从恶意样本与网络行为两方面进行威胁标记。目前，已经为超过 4000 万个样本文件与上亿条网络行为数据提供了所属对应 ATT&CK 技术项的标注。

恶意样本类威胁标记依靠样本的动静态分析结果，如下所示自启动执行（T1547）依赖沙盒动态分析结果标注、加密数据（T1486）依赖静态判黑结果标注。而网络行为类威胁标记则依靠其对应的业务含义进行标注。

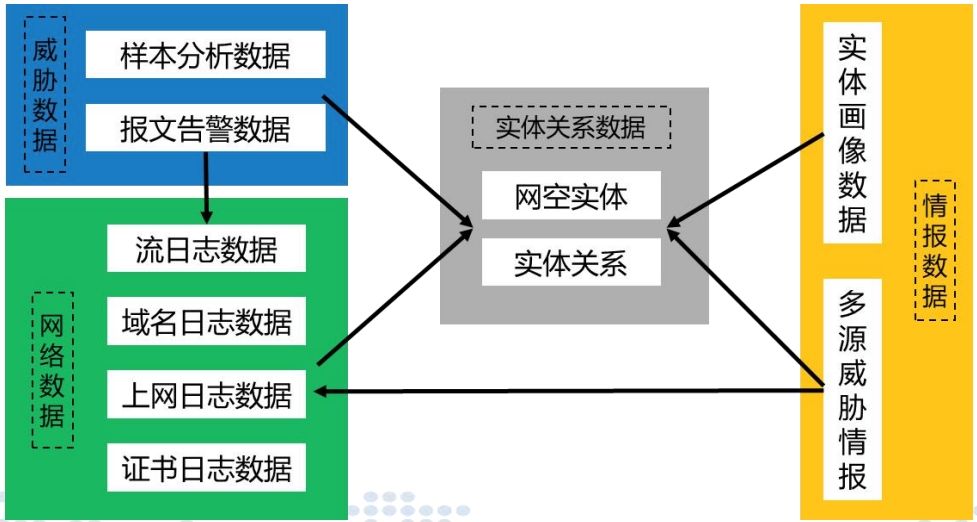
T1547 自启动执行	T1486 加密数据
修改注册表 CurrentVersion\Run	杀软检测结果包含 Ransom
修改注册表 CurrentVersion\RunOnce	杀软检测结果包含 ransom
修改注册表 CurrentVersion\RunEx	杀软检测结果包含 Crypt
修改注册表 CurrentVersion\RunServices	杀软检测结果包含 crypt

T1566 钓鱼
网页仿冒-银行类网页仿冒-仿冒网站监测-XX银行
网页仿冒-银行类网页仿冒-仿冒网站监测-XX银行

多源数据运营 - 网空实体与关系

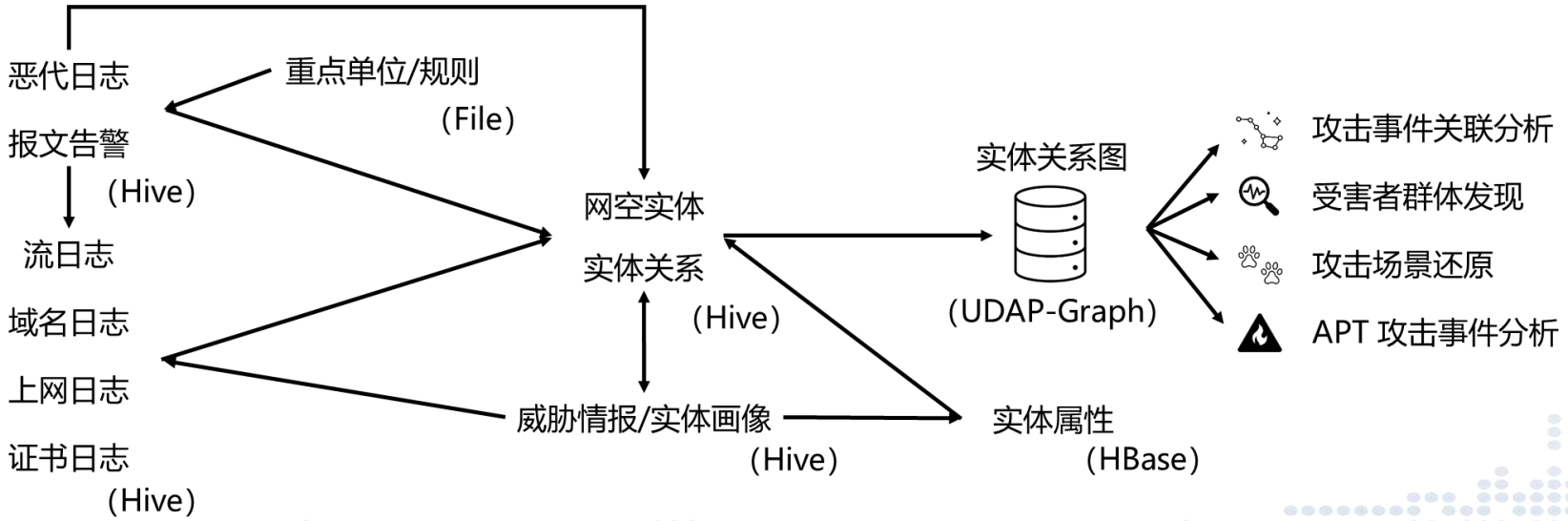
利用多种类、多来源的网络安全数据进行综合关联，构建形成网空实体关系数据。

利用威胁数据（报文告警、文件深度分析）与情报数据（威胁情报）作为起点，筛选重点关注的威胁或重点关注的目标相关的数据，与各种网络痕迹数据相关联，汇总得到网空实体与实体在网络空间中的关联关系。



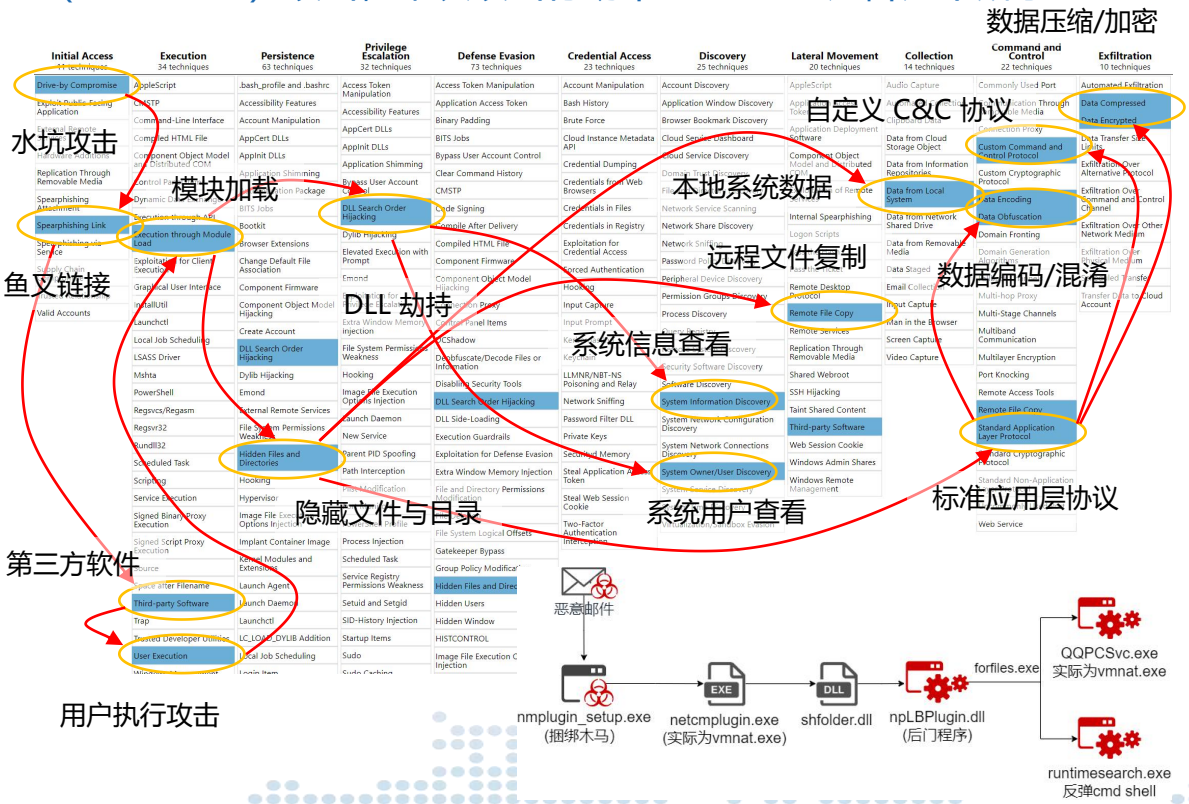
多源数据运营 - 数据处理流转

为了解决安全监测日志碎片化程度高，安全事件关联分析效率低下问题，提取重点单位和威胁情报相关的网络实体属性及关联关系，支持基于实体关系图数据快速发现威胁事件，及时获取事件脉络，为攻击场景还原和受害者判定提供决策依据。



攻击场景还原 - 攻击过程还原

利用 ATT&CK 框架串联攻击事件中碎片化的攻击痕迹，还原攻击场景。监测发现某地某中心遭受 DarkHotel（APT-C-06）攻击，本次攻击行动中 ATT&CK 矩阵如下所示：



完整攻击过程：

1、攻击者渗透攻陷某中心单位的 OA 系统，部署恶意软件构建水坑后向相关人员发送包含恶意软件下载地址的钓鱼邮件。

2、伪装成网易邮箱插件的恶意软件被有关人员下载执行后，通过“白加黑”方式启动加载恶意 DLL 文件。

3、恶意软件收集失陷主机相关系统信息，加密后保存到文件中。

4、将保存失陷主机信息的文件回传到攻击者控制的 C&C 服务器。等待获取攻击者下发后续执行命令，C&C 信道通过 AES 加密传输。

5、执行结果反馈至 C&C 服务器。

组织威胁狩猎 - TTP 描述

利用 ATT&CK 网空威胁框架可以对攻击组织所使用的攻击技术手段进行更加全面的描述和深入的刻画，从 IOC 指标层级走向攻击技战术（TTP）层级。以 DarkHotel 为例，DarkHotel（APT-C-06）是一个疑似来自半岛方向的攻击组织，自从 2004 年就一直活跃，主要攻击目标集中在东亚，包括日本、中国、俄罗斯与朝鲜。也经常针对公共服务、高科技和汽车等行业发起攻击，该组织能力较强能够为攻击行动定制开发恶意软

DarkHotel 常用攻击手段：

1、水坑攻击

2、近源攻击（WiFi 攻击）

3、供应链攻击

4 、钓鱼攻击

5 、P2P 攻击

DarkHotel 常用攻击工具：

1、Inexsmar

2、Tapaoux

3、Karba

4、Pioneer

5、Asruex

DarkHotel 常用漏洞：

1、CVE-2015-8651

2、CVE-2012-0158

3、CVE-2010-2883

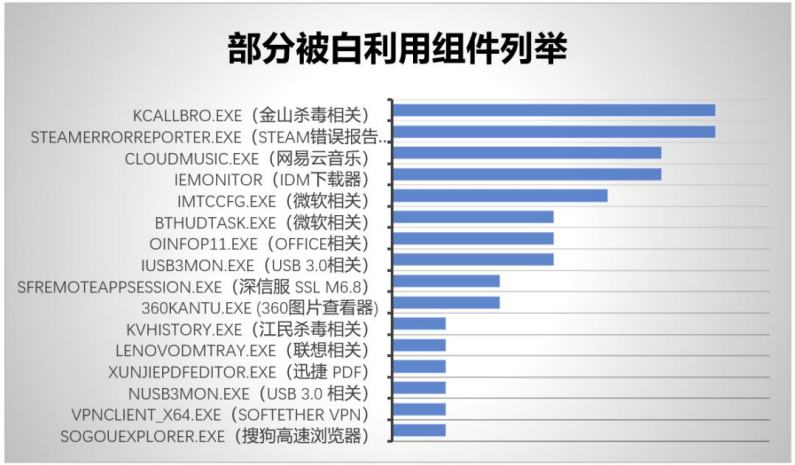
4、CVE-2016-4171

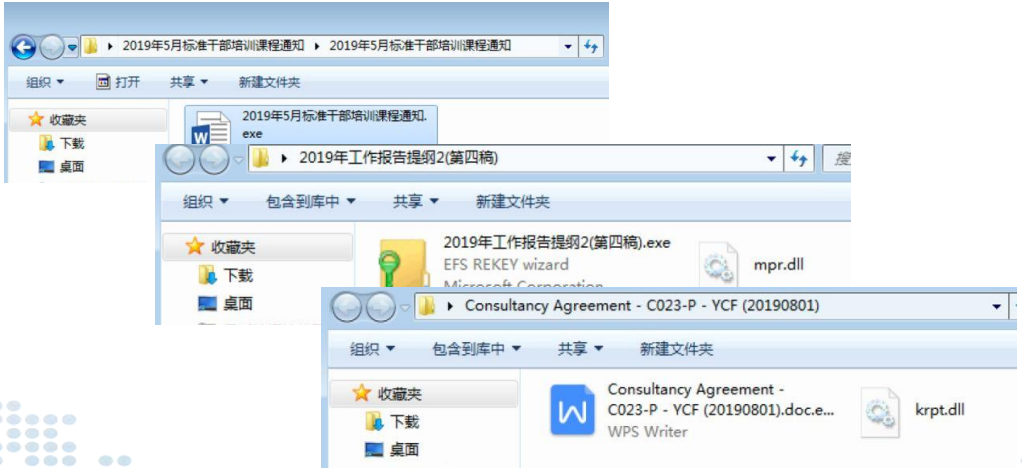
5、CVE-2018-817

组织威胁狩猎

通过将掌握的攻击组织常用技战术手段从低层的 IOC 类威胁指标扩展到高层的 TTP 类，这些更稳定、更不易改变的攻击行为特征可以在 ATT&CK 框架的统一描述下帮助支撑威胁狩猎。

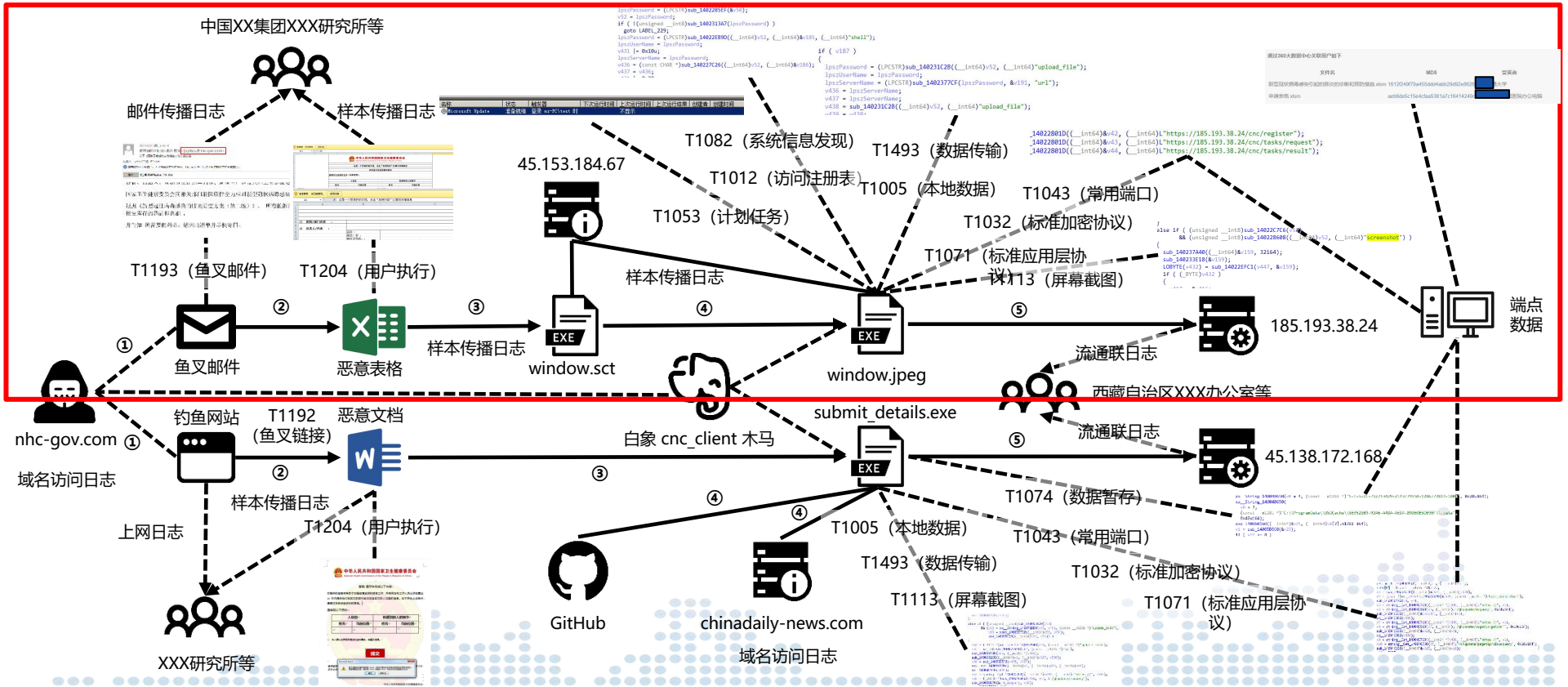
例如，海莲花（APT 32）经常使用“白加黑”的方式加载载荷，也就是利用 DLL 搜索顺序劫持（T1038）技术项。根据对该技术项的检测覆盖，以及白利用组件非常见路径且加载海莲花常用黑 DLL 组件（如其常用的 Cobalt Stike Beacon 或 Denis RAT 木马）、样本文件来源于 SFX 自解压程序等海莲花组织其他攻击特征，可以在端点遥测数据或沙盒动态数据中狩猎海莲花的攻击行动。





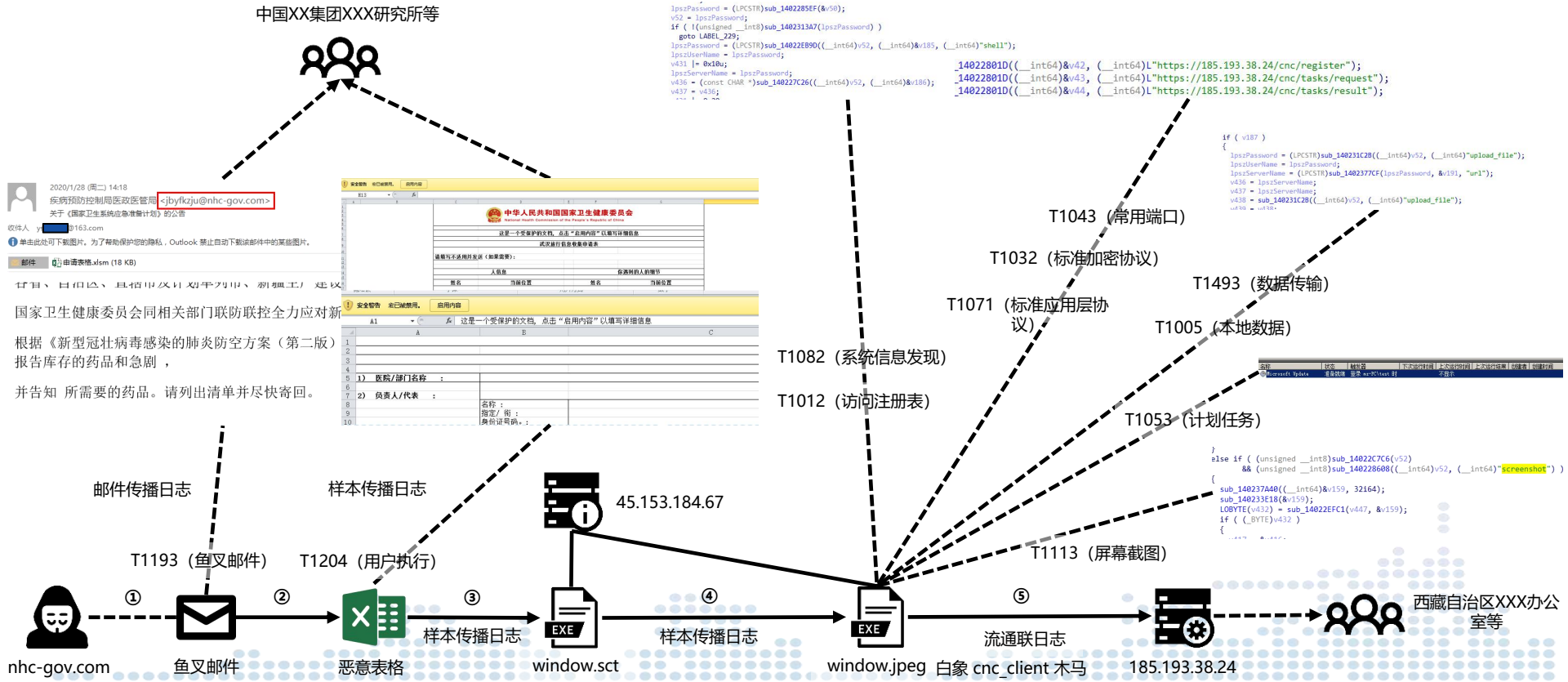
案例

“白象”组织利用新型冠状病毒相关题材，冒充国家卫生健康委员会、疾病预防控制局医政医管局对我国部分行业单位进行攻击。诱使用户执行诱饵文档后通过下载并执行远控木马，实现对受害用户的远程控制和信息窃取。



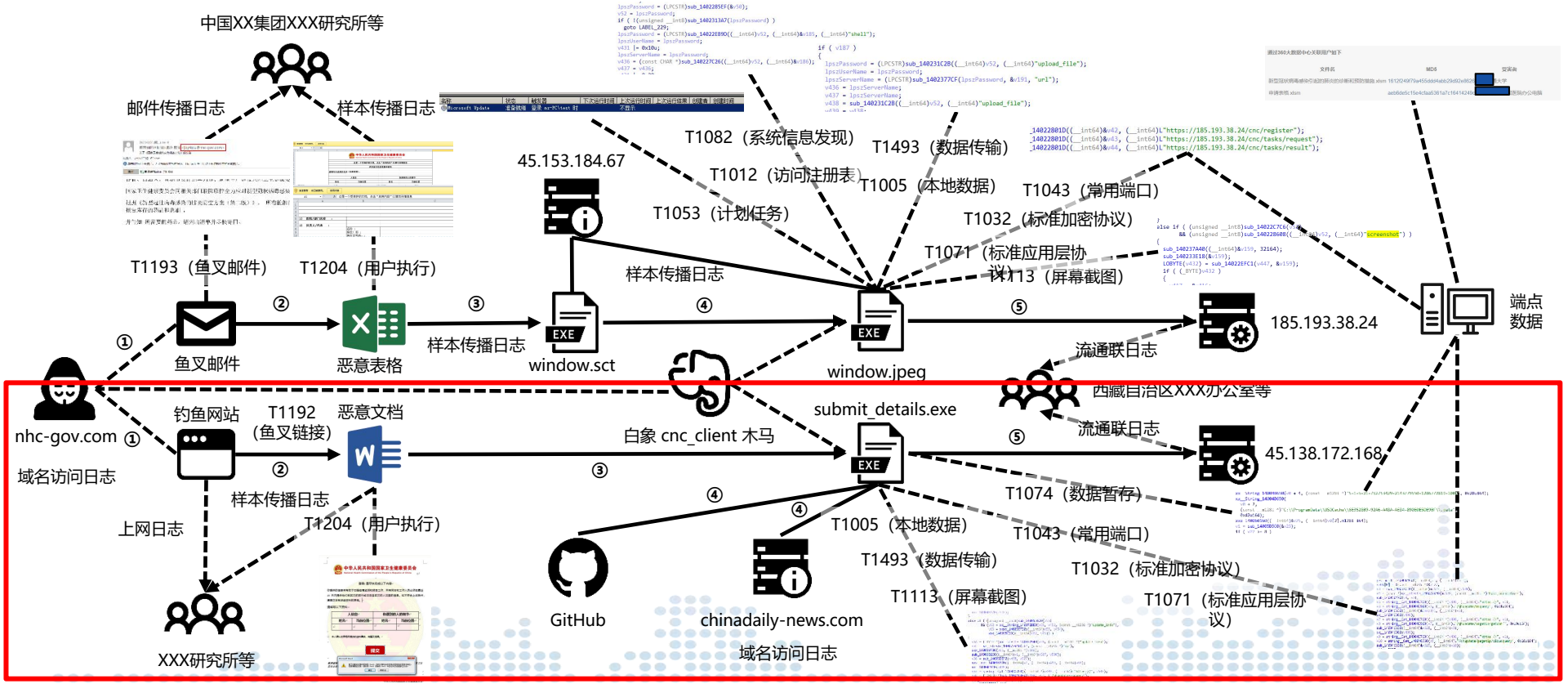
案例

攻击者仿冒国家卫生健康委员会、疾病预防控制局医政医管局，以“关于《国家卫生系统应急准备计划》的公告”为主题向多个攻击目标发送钓鱼邮件，以附件形式投放名为“申请表格.xlsm”、“武汉旅行信息收集申请表.xlsm”等恶意文档



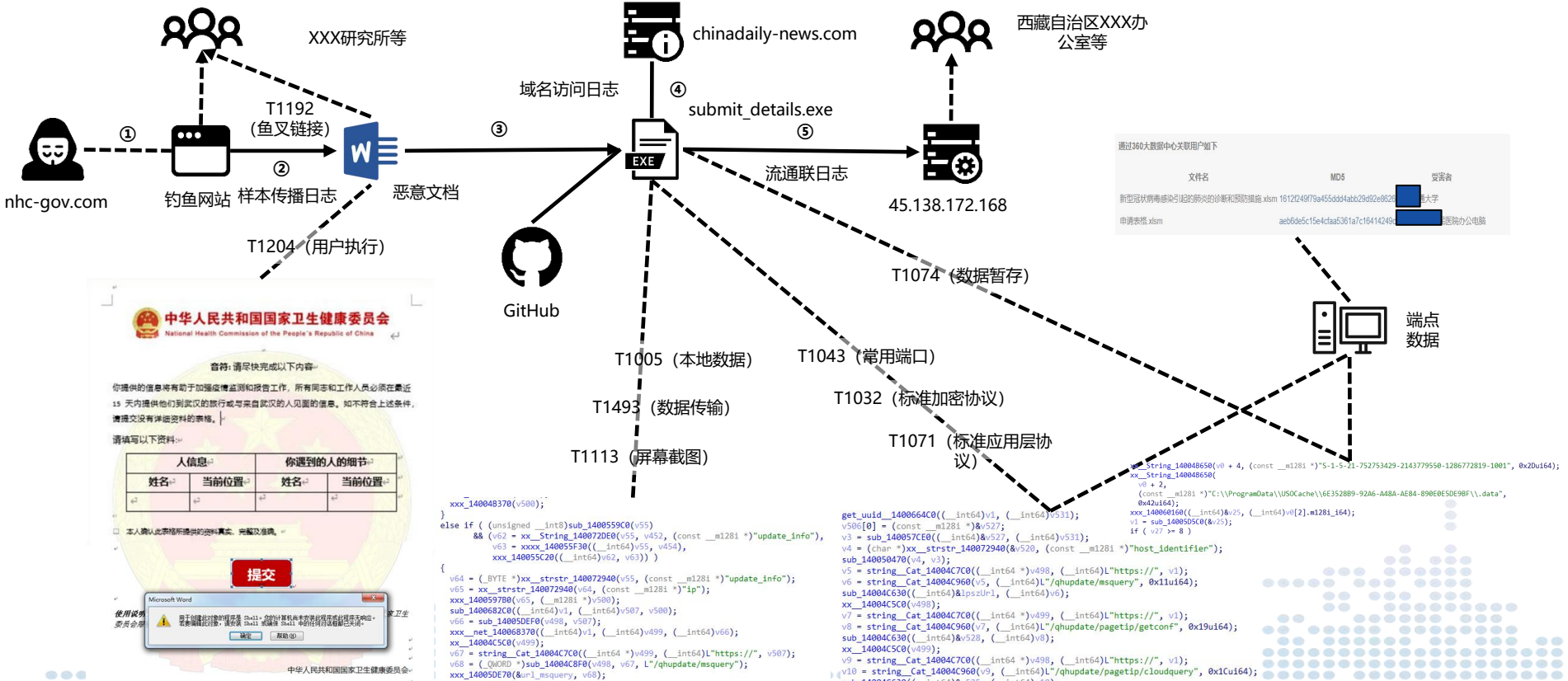
案例

“白象”组织利用新型冠状病毒相关题材，冒充国家卫生健康委员会、疾病预防控制局医政医管局对我国部分行业单位进行攻击。诱使用户执行诱饵文档后通过下载并执行远控木马，实现对受害用户的远程控制和信息窃取。



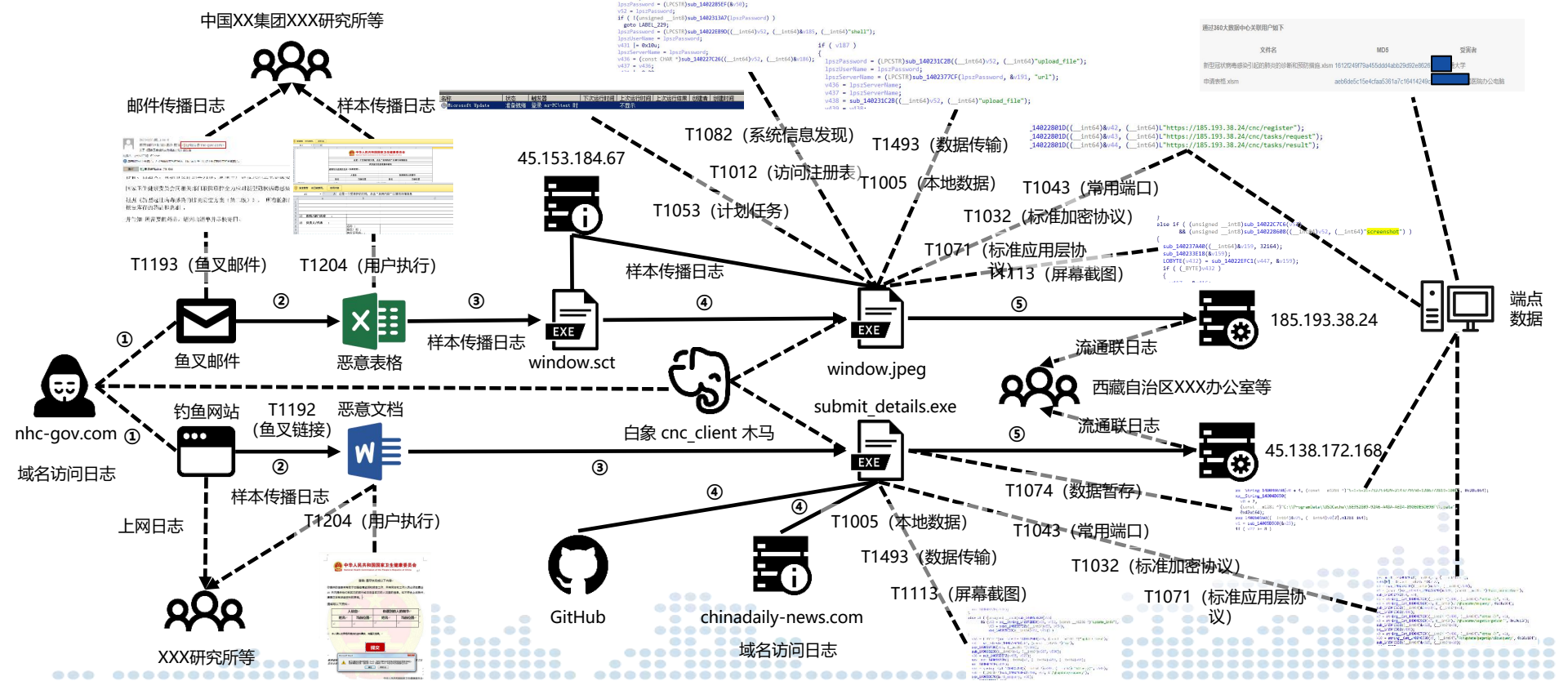
案例

诱饵文档冒充国家卫生健康委员会收集疫情相关信息，引诱用户点击提交按钮，触发 shell.explorer 加载对象通过 GitHub 下载恶意软件。该恶意软件以国徽为图标，诱导用户点击执行。



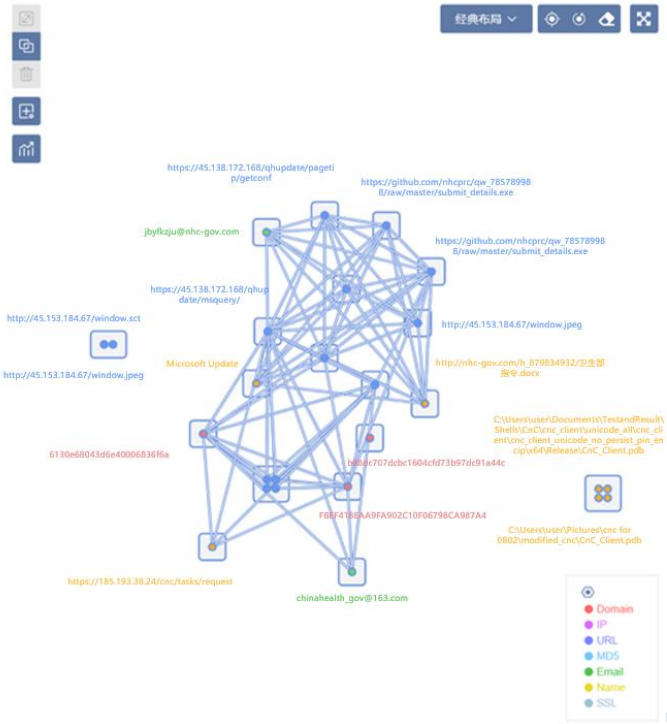
案例

“白象”组织利用新型冠状病毒相关题材，冒充国家卫生健康委员会、疾病预防控制局医政医管局对我国部分行业单位进行攻击。诱使用户执行诱饵文档后通过下载并执行远控木马，实现对受害用户的远程控制和信息窃取。



攻击行动中所有涉及到的完整 ATT&CK 矩阵与所有相关的攻击基础设施等网空实体在关联分析图谱中如下所示。

关联分析图谱（系统截图）



完整 ATT&CK 矩阵（系统截图）

初始访问	执行	持久化	权限提升	防御逃逸	凭证访问	发现	横向移动	收集	渗出	C&C	影响
通过式下载	命令和脚本解释器	帐户操作	滥用提权控制机制	滥用提权控制机制	暴力破解	帐户发现	组件对象模型和分布式COM	存档收集的数据	自动渗透	应用层协议	帐户访问权限删除
利用面向公众的应用程序	组件对象模型和分布式COM	BITS任务	访问令牌操纵	访问令牌操纵	密码存储中的凭证	应用程序窗口发现	远程服务的利用	音频捕获	数据传输大小限制	常用端口	数据销毁
外部远程服务	利用客户执行	引导或登录自动启动执行	引导或登录自动启动执行	BITS任务	利用凭证访问	浏览器书签发现	内部鱼叉	自动收集	通过替代协议渗透	通过可移动媒体进行通信	加密数据以产生影响
部外硬件	图形用户界面	引导或登录初始化脚本	引导或登录初始化脚本	反混淆/解码文件或信息	强制认证	云服务仪表板	输出工具转移	剪贴板数据	通过C2通道渗透	数据编码	数据处理
钓鱼	进程间通讯	浏览器扩展	创建或修改系统过程	直接移动司	输入捕捉	云服务发现	远程服务会话劫持	数据暂存	通过其他网络介质渗透	数据混淆	污染
通过可移动媒体复制	原生API	关闭的客户调软件二进制	事件触发执行	执行协作	中间人	域信任发现	远程服务	来自云存储对象的数据	物理介质上的渗出	动态解析	磁盘擦除
供应链为响	计划任务	创建帐号	利用特权升级	属的进通利用	修改身份验证过程	文件和目录发现	通过可移动媒体复制	信息存储库中的数据	通过Web服务渗透	加密信道	端点拒绝服务
信任的关系	脚本编写	创建或修改系统过程	组策略修改	文件和目录权限修改	网络嗅探	网络服务扫描	共享Webroot	来自本地系统的数据	计划传输	后备信道	固件损坏
有效帐户	共享模块	事件触发执行	劫持执行流程	组策略修改	操作系统凭证转储	网络共享发现	软件部署工具	来自网络共享驱动器的数据	将数据转移到云帐户	入口工具转移	禁止系统恢复
	软件部署工具	外部远程服务	路径拦截	隐藏产物	窃取应用程序访问令牌	网络嗅探	污染共享内容	来自可移动媒体的数据		多阶段信道	网络拒绝服务
	source命令	劫持执行流程	工艺注入	劫持执行流程	窃取Web会话Cookie	密码策略发现	使用备用验证材料	邮件收集		多信道通讯	资源劫持
	系统服务	Hypervisor	计划任务	侵蚀防御	窃取或办造Kerberos票证	外围设备发现		输入捕捉		出应用层协议	服务停止
	用户执行	植入容器镜像	有效帐户	掩除主机上的利用指标	双因素身份验证拦截	权限组发现		浏览器中间人		非标准端口	系统关机/重启
	Windows管理规范	Office应用程序启动		间接命令执行	未受保护的凭证	流程发现		中间人		协议隧道	
		路径拦截		LC_MAIN劫持		查询注册表		屏幕截图		代理	
		操作系统启动		伪装		远程系统发现		视频捕捉		远程访问软件	
		冗余访问		修改身份验证过程		软件发现				流量信号	
		计划任务		修改云计算基础架构		系统信息发现				Web服务	
		服务器软件组件		修改注册表		系统网络配置发现					
		流量信号		滥用的文件或信息		系统网络连接发现					
		有效帐户		操作系统启动		系统所有者/用户发现					
				工艺注入		系统服务发现					

案例

根据攻击者攻击过程和使用的攻击资源进行分析，查找境内疑似受害者。共分析发现 54 个被攻击目标，涉及政府、军工、研究院校等重要行业的 20+ 个单位，确定了分布在全国 14 个省份的 40+ 个疑似失陷主机。

境内疑似被控分布情况（系统截图）

CNCERT/CC
国家互联网应急中心

Q&A

Tel:
010-82990999（中）
010-82991000（英）

Web:
www.cert.org.cn

E-mall
cncert@cert.org.cn