网络空间威胁对抗与态势感知研讨会
暨 第六届安天网络安全冬训营

接触式攻击和电磁装备在网空攻防中所带来的威胁

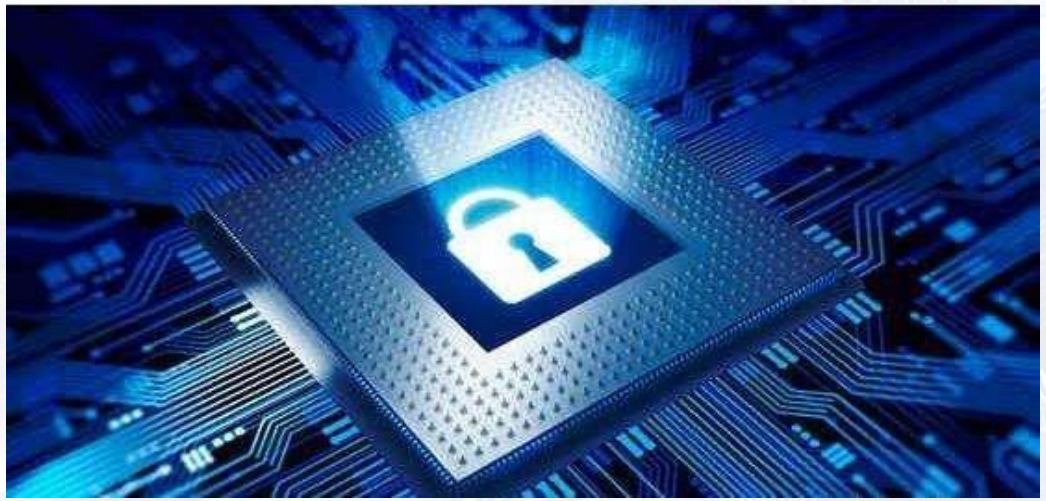
安天微电子与嵌入式安全研发部

战术型态势感知指控积极防御
协同响应猎杀威胁运行实战化

铁流鏖戰

提纲

- 在网空攻防中物理攻击的增益效果
- 某方网络装备体系之硬件篇
- 网空威胁之硬件攻击推演



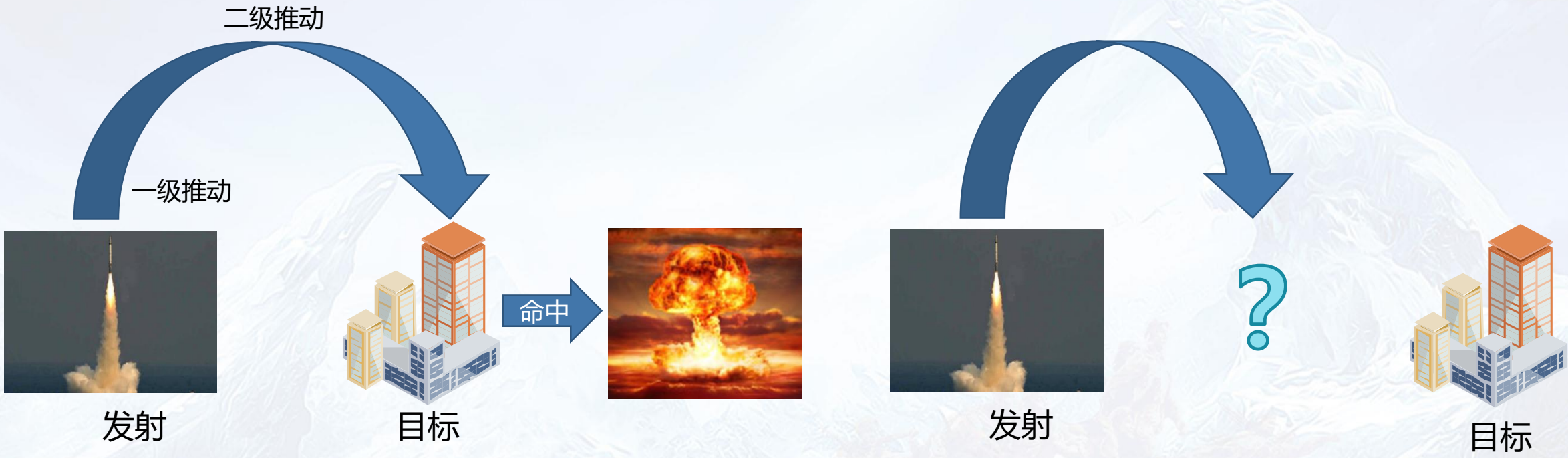
01 在网空攻防中物理攻击的增益效果

物理攻击能够对网络攻击武器的攻击效果形成巨大增益

NSA / CSS 技术网络威胁框架 v1 - 全景视图

管理			准备		交互		存在						影响					持续进程			
规划	资源开发	研究	侦察	分级	传播	漏洞利用	安装和执行	内部侦察	提权	凭证访问	横向运动	持续性	监控	渗漏	修改	拒绝	破坏	分析，评估和反馈	c2	指挥与控C2	规避
确定战略和目标	开发能力	识别情报差距	网络抓取	创建中点	钓鱼邮件/附件	定位应用程序漏洞	写入磁盘	账户枚举	使用合法凭证	凭证	应用部署软件	使用合法凭证	利用弱访问控制	脚本渗漏	破坏加密	分布式拒绝服务（DDOS）	部分磁盘/操作系统删除（损坏）	改进定位	常用端口施	使用合法凭证	采用逆向工程措施
分析任务	获得融资	识别能力差距	网络映射	将漏洞添加到应用程数据文件	带有恶意链接的钓鱼邮件	目标操作系统漏洞	在内存代码中	文件系统枚举	辅助功能	网络嗅探	定位应用程序漏洞	访问功能	跟踪访问	压缩数据	改变数据	加密数据以使其不可用	磁盘/操作系统删除	进行效果评估	不常用端口	二进制填充	采用反取证措施
制定运营计划	员工和培训资源	召集人才	使用社交媒体	分配运营基础设施	网站	远程针对应用程序漏洞	解释脚本	组权限枚举	启动时自动加载	键盘记录	目标操作系统漏洞	启动时自动加载	被动收集	节流数据	造成物理影响	拒绝服务/中断	数据删除（部分）		标准应用层协议	禁用安全产品	模仿合法的流量
选择战略目标	建立稳固伙伴关系		扫描	感染或种子网站	可移动媒体	社会工程学	二进制替换	本地网络连接枚举	图书馆搜索劫持	社会工程学	使用登录脚本	图书馆搜索劫持	启动其他操作	位置数据	克隆数据	系统降级	数据删除		标准的非应用层协议	扰乱,安全产品	避免数据大小限制
获得执行操作的批准	获取运营基础设施		选择战术目标	预定位有效载荷	SQL注入	虚拟化攻击	命令行	本地网络设置枚举	创建新的服务	密码破解	利用对等连接	创建新的服务		C2通道上的Exfil	更改系统进程的运行状态		毁坏硬件		自定义应用层协议	访问原始磁盘	编码数据
发布业务任务	创建僵尸网络		调查	建立物理接近度	DNS/缓存	破坏加密	由用户启用	操作系统枚举	路径拦截	添加或修改凭证	远程交互式登录	路径拦截		非C2通道上的Exfil	改变过程结果				使用链接协议	阻止主机上的指示器	加密数据
	种子供应链		TCP指纹识别		虚拟化攻击	利用弱访问漏洞	流程注入	所有者/用户枚举	计划任务	劫持活动证书	使用远程管理服务	计划任务		Exfil通过其他网络媒介	更改机器到机器（MtM）通信				使用可移动媒体	修改恶意软件以避免检测	
			横幅抓取		连接流促网络设备	远程	配置修改以促进发射	进程枚举	替换服务二进制	在文件中查找凭证	远程服务	替换服务二进制		来自本地系统	Deface网站				后备通道	删除记录的数据	
			社会工程学		可信网站	缓冲区溢出漏洞	使用可信应用程序执行不受信代码	软件枚举	连接修改		通过可移动媒体复制	链接修改		从网络资源收集					多频段通信	操作可信进程	
			凭证流域		合法的远程访问	利用漏洞	计划任务	服务枚举	操作可信进程		共享webroot	编辑文件类型关联		计划转移					使用对等链接	流程注入	
			串扰（数据发射）		设备交换（跨域违例）	启动0日攻击	通过服务控制器执行	窗口枚举	流程注入		污染共享平台	修改BIOS		临时转移					建立对等网络	模拟合法文件	
			识别密码		利用CDS或MLS错误配置	规范化	第三方软件	键盘记录	定位应用程序漏洞		远程文件共享	安装hypervisor rootkit		Exfil超过物理介质					信标	将文件出储存在非常规位置	
					物理网桥	劫持	使用远程管理服务	屏幕截图	目标操作系统漏洞		中继通信	使用登录脚本		串扰（数据发射）					加密通信	混淆数据	
					自动传输可信服务	重播	OS API以促进发射	激活记录	修改服务配置		通过哈希	编辑MBR		编码数据					使用多层加密	使用Rootkit	
					遍历CDS或MLS	协议滥用	转移工具套件				通票	修改现有服务		破坏加密					使用标准加密	使用可信应用程序执行不守信代码	
					供应链/可信任来源的妥协	利用信任关系						修改服务配置		遍历CDS或MLS					使用自定义加密	软件包	
					无线接入							后门							自动使用C2	使用签名内容	
					妥协通用网络基础设施														手动使用C2	签署可疑内容	
					短信服务（SMS）															删除套件	
					快速响应（QR）代码															基于环境的行为	
					编码数据															延迟活动	
					木马																

传统武器的达到与控制问题

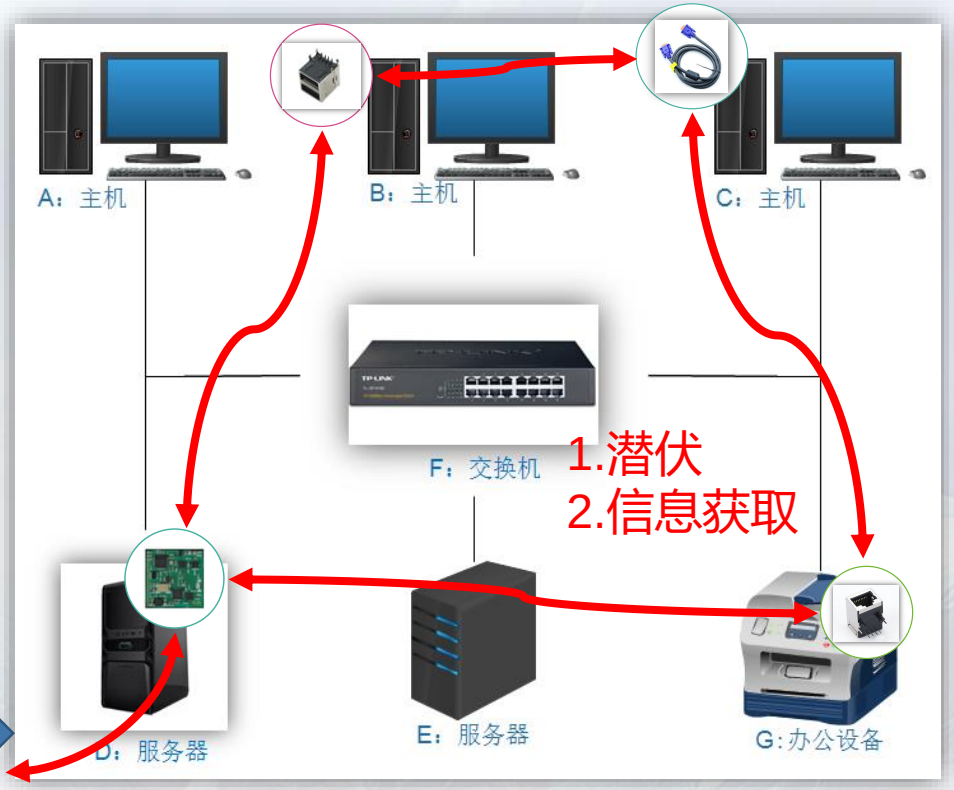


在射程范围内摧毁目标

在射程外——无效装备

网络攻击的达到、控制与回传问题

链路不存在



远程网络攻击

接触式攻击+电磁装备
构建立新的可达链路

隔离网

物理手段对网络攻击带来了哪些增益

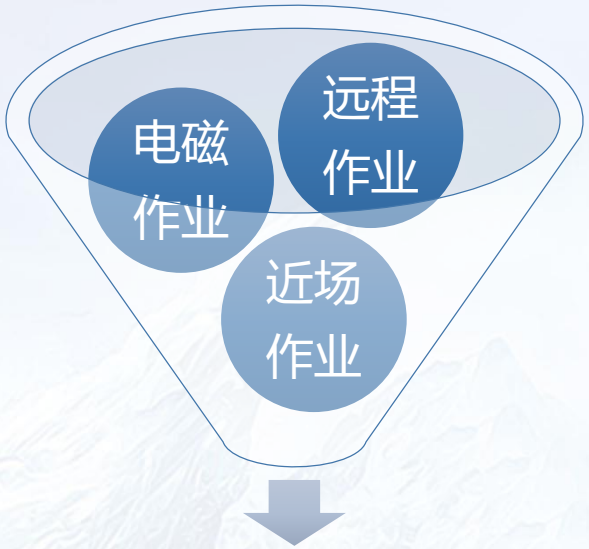
A-到达问题	当网络不能达到时，物理手段是可以起到铺垫作用
B-控制问题	可辅助网络攻击提升对目标的多种维度的控制能力
C-数据回收问题	在网络不可使用时，能够通过人或装备构建的第二信道完成数据的回收

情报作业	攻击作业	影响作业	持久化作业
A B C	A B C	A B C	A B C

物理攻击对网络攻击的叠加和增益

管理	准备	交互	存在						影响					持续进程		
规划	侦察	分级	传播	漏洞利用	安装和执行	内部侦察	提升	凭证访问	横向运动	持续性	监控	渗漏	修改	拒绝	破坏	分析、评估和反馈	C2	躲避
资源开发	网络抓取		木马		用户启用		账户枚举		启动自动加载		利用弱控制访问	从物理媒介偷出	更改数据	加密数据使其不可用		表现效果评估	备用通道	
研究	扫描		漏洞		键盘记录		污染共享内容		编辑MBR		部分磁盘/操作系统删除（损坏）					限制主机指示器		
	……		……		……						……					……		
	1.人+软件+内网操作 2.人+硬件+内网操作		1.人+直接植入 2.人+供应链植入 3.人+硬件设备植入		1.人+直接操作 2.硬件设备 3.硬件设备构建第二信道						1.人+直接操作 2.硬件设备信号层支持 3.硬件设备构建第二信道					1.人+现场效果评估 2.硬件设备信号层支持 3.硬件设备构建第二信道		

需要防御的不只是漏洞利用和恶意代码



多种手段复合作业

- 近场作业
  - 最基本的、可靠的攻击手段
  - 信息获取的前置手段
  - 某些设备必备的攻击手段
- 电磁作业
  - 融合进场作业的攻击手段
  - 针对设备硬件体系的专用攻击手段
  - 特有信息传递方法
- 远程作业
  - 网络攻击的手段
  - 前期预置设备的控制和数据回传手段

02 某方网络装备体系之硬件篇

物理攻击是整个网空威胁不可缺少的一部分

某方网络装备体系


端点目标
网络场景
作业方式
支撑体系
桌面计算机
移动终端
服务器
微型计算机
网络设备
网络安全设备
信号设备
人
供应链
劫持
仓储
摆渡
资源库
技术库
攻击&分析平台
配套工具
其它

某方三位一体、三个特点

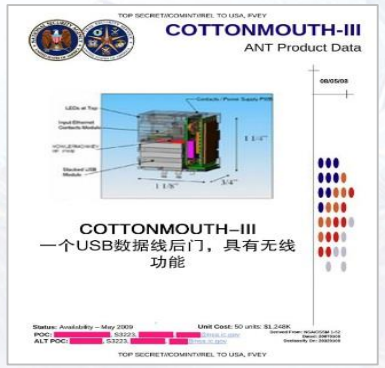
- **多种投放方式**
  - 传统情报+物流链
  - 供应链
  - 人工（黑带）
- **多种回传控制方式**
  - 远程控制
  - 近场控制
  - 构建第二信道
- **多点作业**

端点——针对外设和接口的攻击装备

显示器

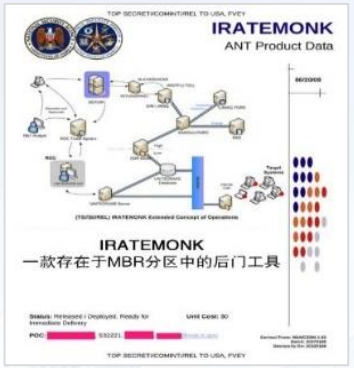
键盘

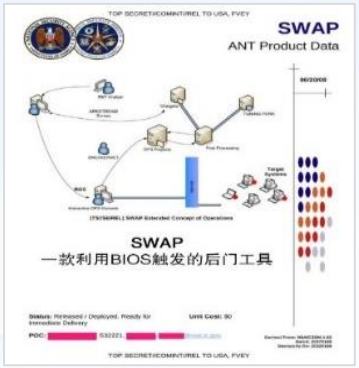
通用串行总线

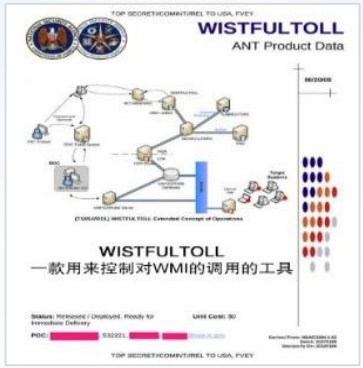


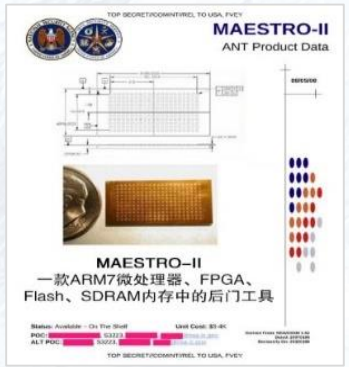
端点——电脑主机、服务器的攻击装备

电脑

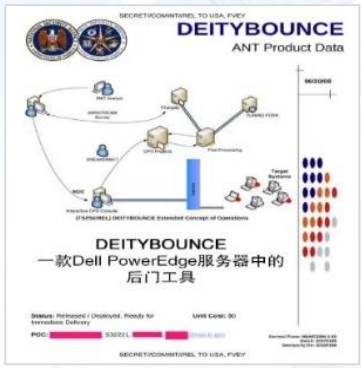


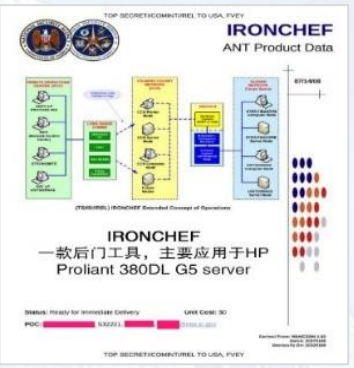






服务器

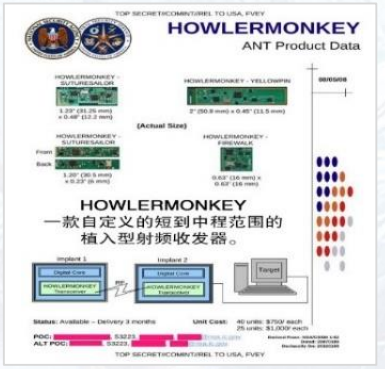




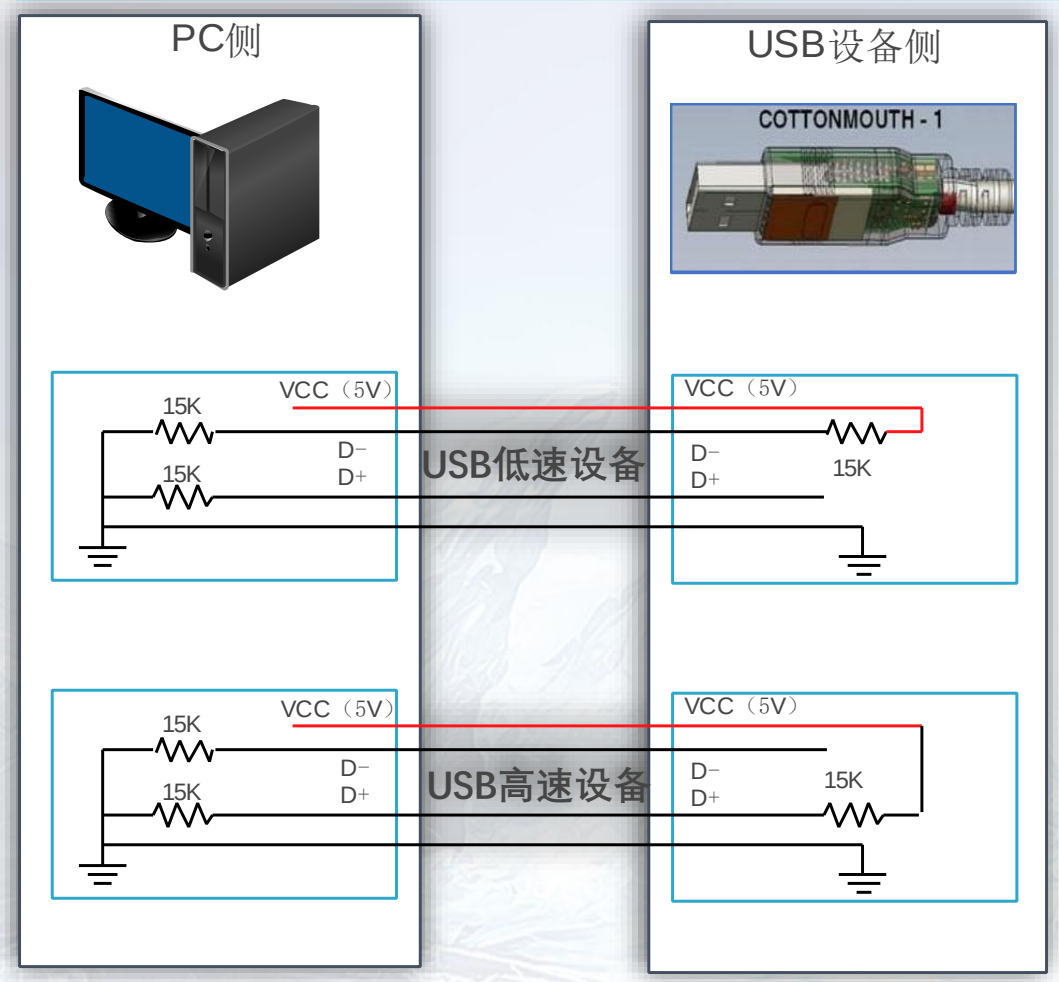
网络攻击、信息传输相关的攻击模块

无线局域网

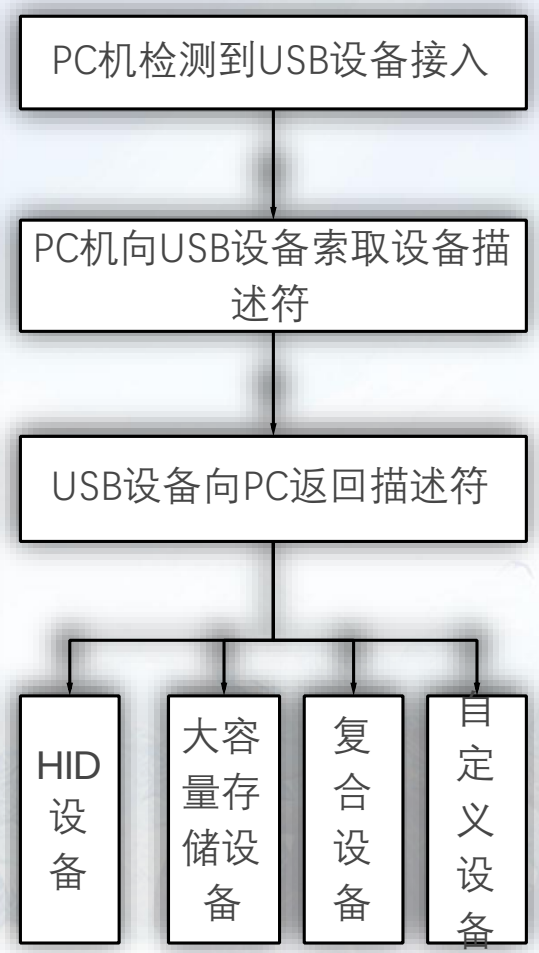
空间设备



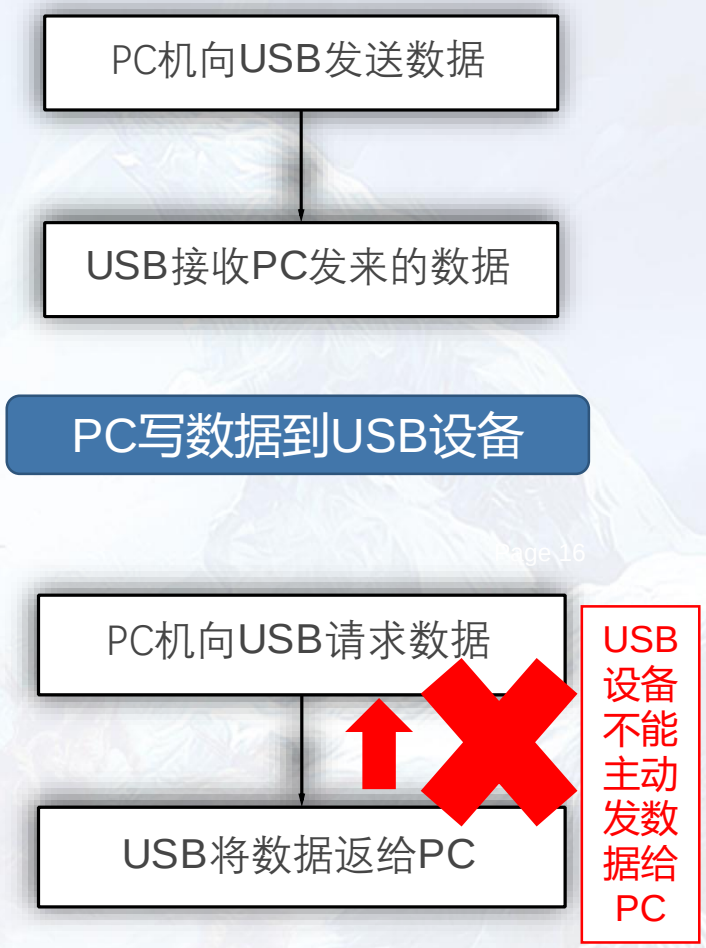
COTTONMOUTH系列装备攻击原理猜想和分析——USB总线工作原理



USB设备接入识别方法



USB设备类型获取



PC读取USB设备数据

COTTONMOUTH系列装备攻击原理猜想和分析——可能的实现方案

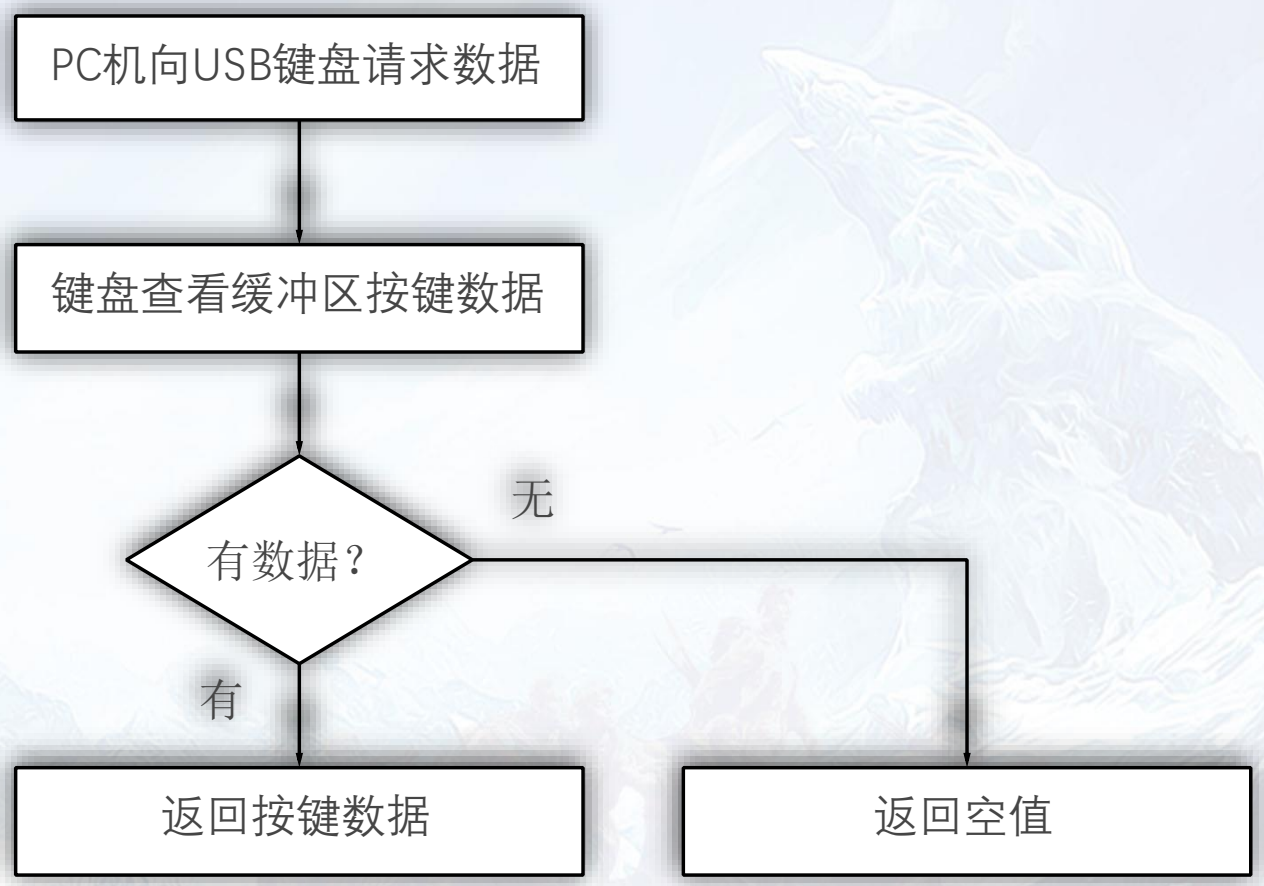
USB设备不能够主动发起对主机的读/写数据传输

需要具备主动攻击的能力	需要具备载荷存储空间	需要具备数据存储空间	需要远程控制访问
USB键盘/鼠标	USB大容量存储设备	USB大容量存储设备	无线传输模块

支持BadUSB和USB大容量存储设备功能的USB复合设备+独立的无线传输模块和软件系统

COTTONMOUTH系列装备攻击原理猜想和分析——USB键盘工作原理

USB键盘识别过程



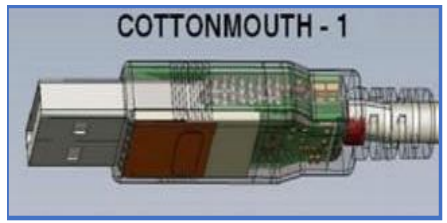
按键数据获取

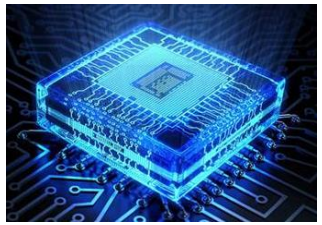
COTTONMOUTH系列装备攻击原理猜想和分析——BadUSB工作原理

①USB键盘设备

②能够主动生成按键序列

工作过程



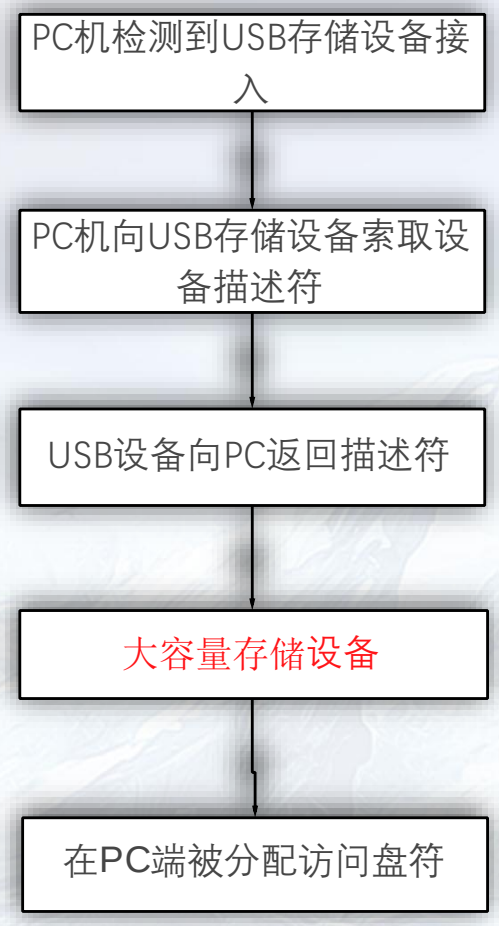


激活条件达成

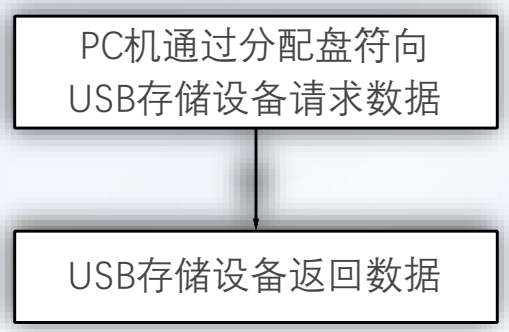
无线远程控制

根据预置条件或控制命令模拟键盘人工输入方式产生具备攻击能力或启动载荷能力的按键序列

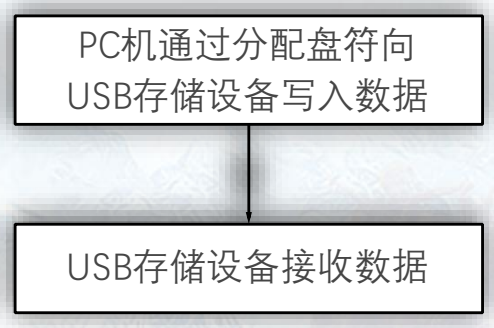
COTTONMOUTH系列装备攻击原理猜想和分析——USB大容量存储设备



USB存储设备识别过程



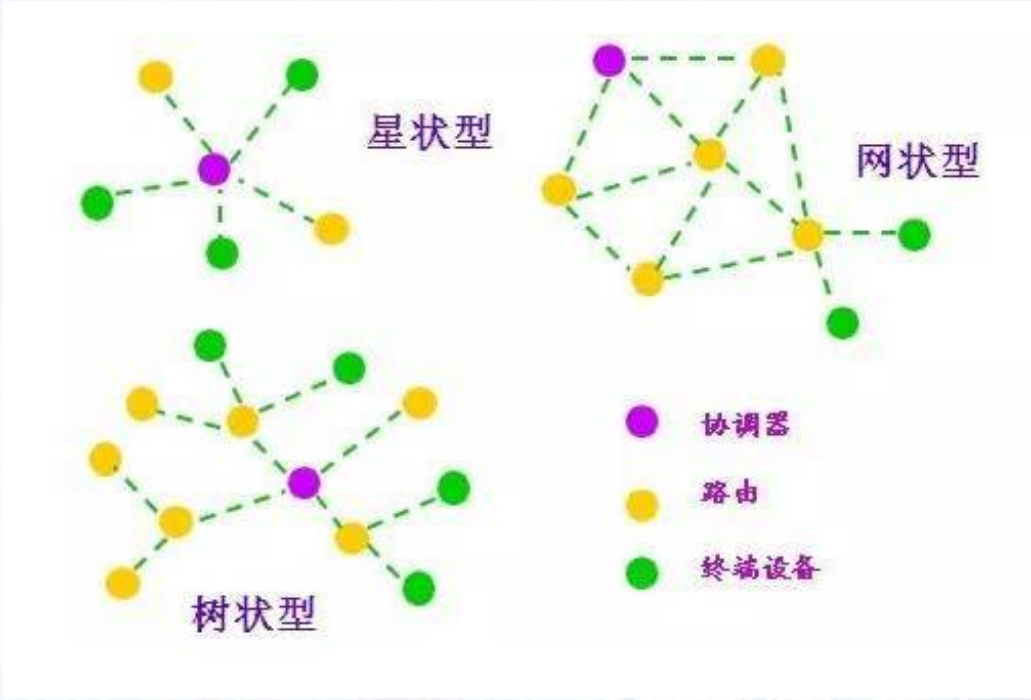
PC写数据到USB存储设备



PC从USB存储设备读数据

专有协议读写操作

COTTONMOUTH系列装备攻击原理猜想和分析——无线工作原理



ZigBee协议在2003年中正式问世

COTTONMOUTH-I是2009年1月可用

COTTONMOUTH系列装备攻击原理猜想和分析——攻击方式

03 网空威胁之硬件威胁推演

来自于硬件的多维度网空威胁

硬件威胁推演场景列表

①隔离网+光盘数据传输攻击推演

②虚拟场景全过程攻击推演

隔离网+光盘数据传输攻击推演

【①隔离网场景介绍】

- 内部独立成网
- 禁止外部网络设备接入
- 封锁主机外部接口
- 禁止使用U盘、移动硬盘等存储设备传递数据
- 使用光盘进行数据传输
- 重要文档使用纸制保存

【②场景分析】

- 数据交换介质
  - 光盘和纸制文档
- 涉及设备
  - 光驱和打印机

【③方案制定】

- USB光驱替换
  - 潜入替换，人员策反替换，供应链路替换
- 打印机软件武器
  - 软件装备结合光驱武器使用

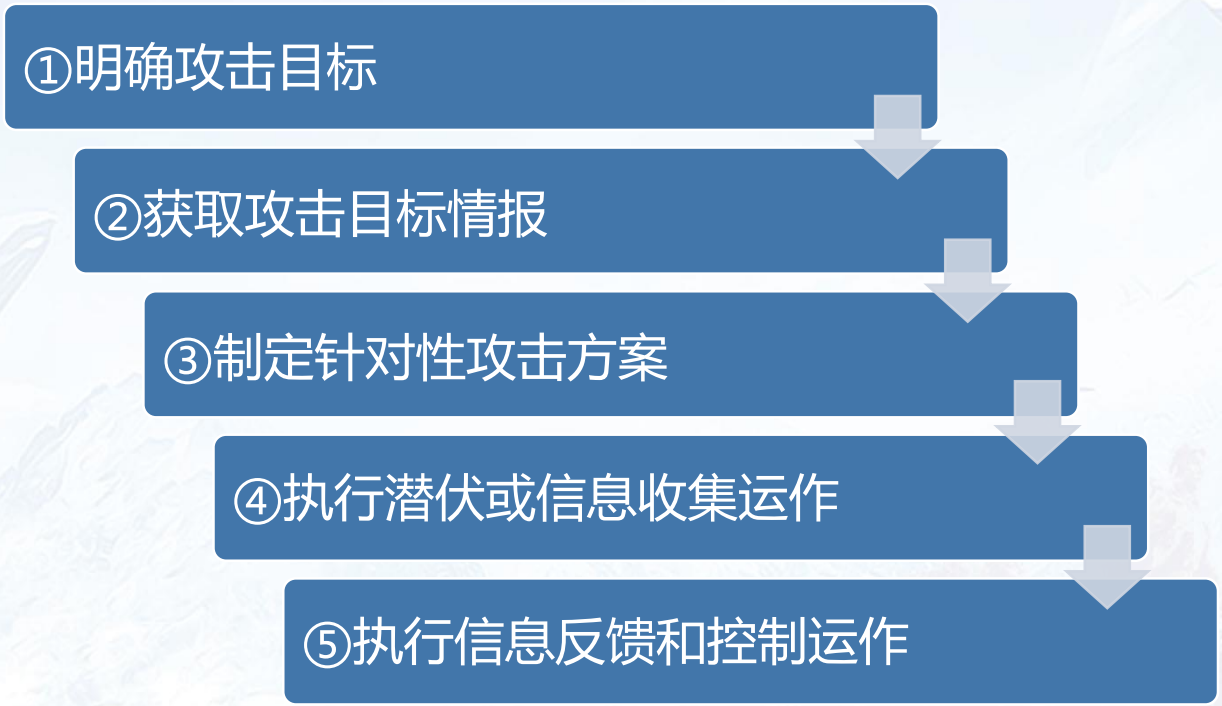
【④武器制造】

- USB光驱
  - 将COTTONMOUTH-I植入同型号光驱中
- 打印机
  - 根据打印机型号使用专用病毒武器，在感染打印机后将所打印文档传给上游主机。

【⑤推演结果】

- 通过USB光驱将打印机专用病毒武器投放到目标网络的打印机设备，然后将打印机所打印过的**文档**传递给上游主机，再使用专有SCSI协议传递给USB光驱，然后通过无线链路将数据传出。

虚拟场景全过程推演——步骤



虚拟场景全过程推演——明确目标和信息收集

保密
办公区

目　　标：**某敏感办公区**

相关信息：

1.封闭办公区，人员出入需要身份确认。

2.有专职的保洁和网管人员。

3.分为物理隔离保密网和常规联网办公网。

4.近期有采购计划，采购清单（电脑、显示器、键盘、鼠标、交换机等）。

5.集中招标采购方式，有公示的供应商列表。

6.供应商以公路、铁路、航空等方式将采购设备送到指定仓库。

虚拟场景全过程推演——方案定制

方案一 人员策反

策反目标：保洁和网管

方案简述：策反目标内部人员，提供针对性工具，由相关人员带入后通过多种方式实现载荷的置入和信息获取。

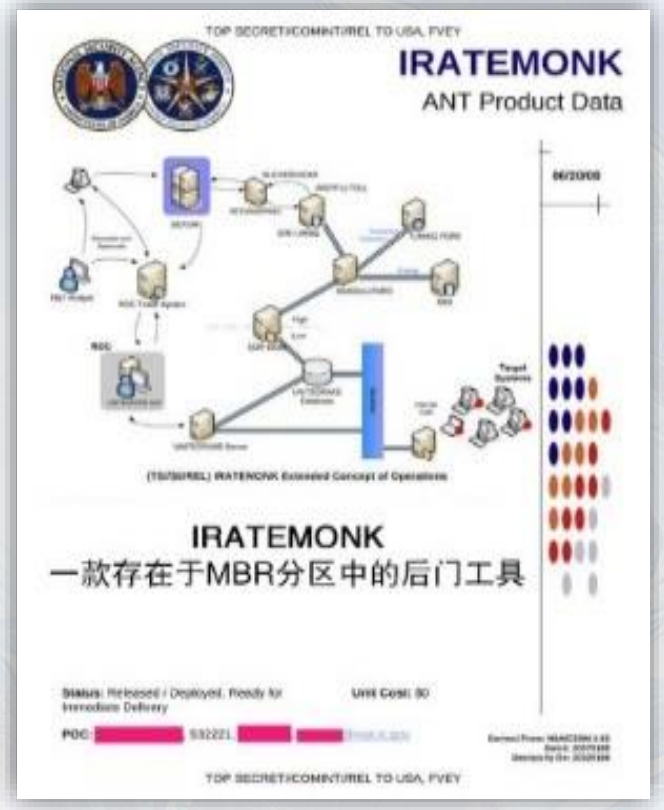
方案二 供应链、物流链植入

植入环境：运输途中

方案简述：根据目标采购设备列表，准备相应的装备，并在设备运输过中进行装备替换和植入。

虚拟场景全过程推演——人员突破方案武器选择

硬件装备



软件载荷

虚拟场景全过程推演——人员突破方案武器使用

COTTONMOUTH-1

RAGEMASTER、 LOUDAUTO

借给工作人使用

接入目标主机直接感染主机

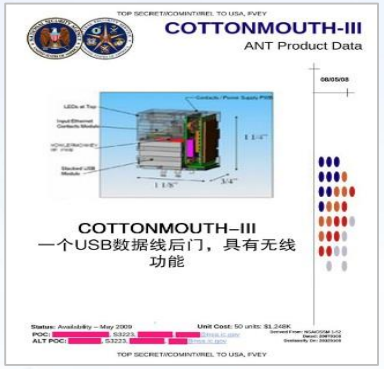
替换现有线缆

伪装 → 突破 → 载荷运行

虚拟场景全过程推演——供应链突破方案武器选择

显示器

通用串行总线



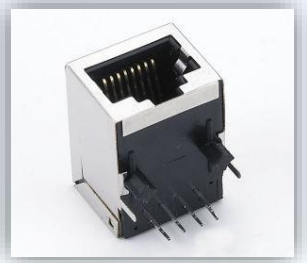
音频

定位和无线数传

键盘

虚拟场景全过程推演——供应链路突破方案武器使用

COTTONMOUTH-III



FIREWALK

SURLYSPAWN

RAGEMASTER、 LOUDAUTO

植入

TAWDRYARD

HOWLEMONKEY

设备整体替换或装备植入

虚拟场景全过程推演——装备潜伏或信息收集

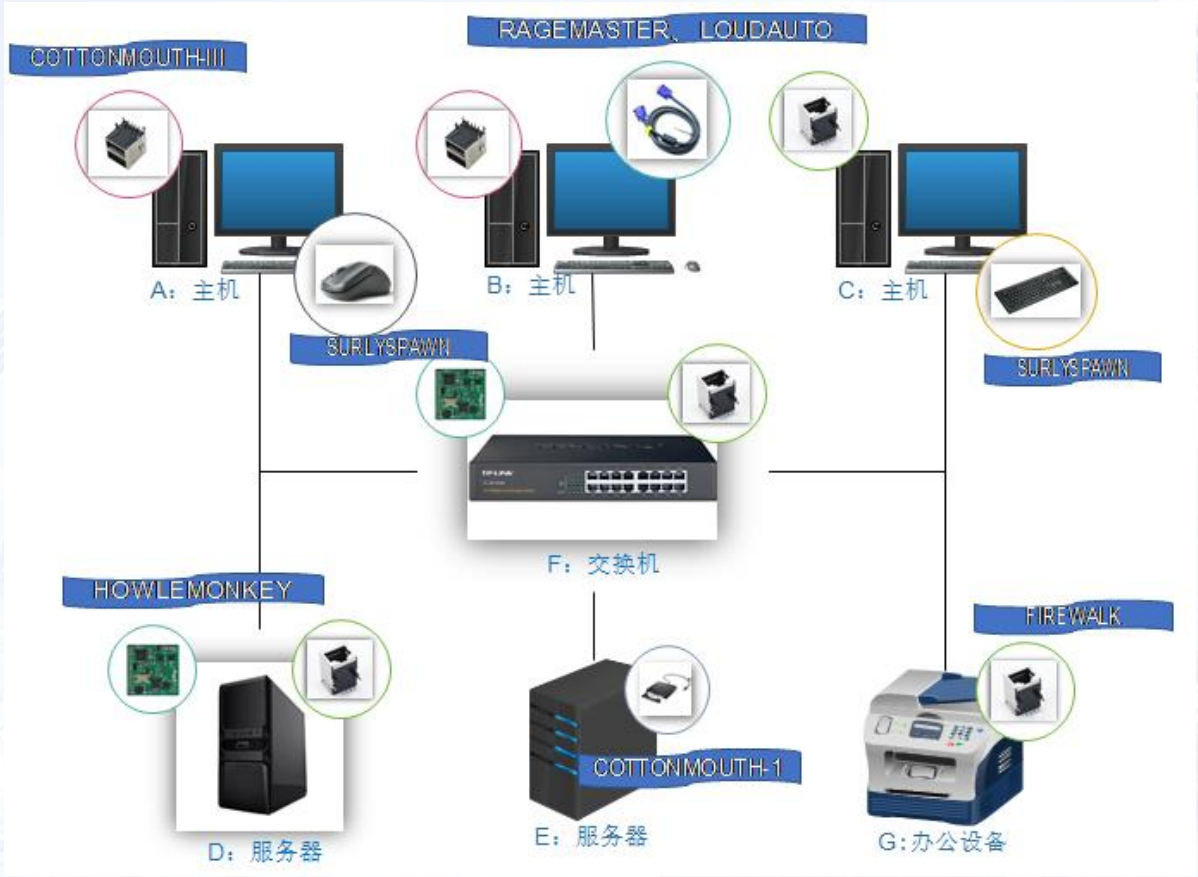
潜 伏

动作描述：

装备和载荷处于静默状态，在激活条件达成后才对目标发起攻击。

激活条件：

1. 设定时间到
2. 关键字触发
3. 远程信号启动
4. *人工启动*



信息收集

动作描述：

按预设的规则完成目标网络内的有效信息收集。

收集内容：

1. 主机信息
2. 网络数据
3. 打印文档内容
4. 屏幕内容
5. ……

虚拟场景全过程推演——控制和反馈

远程控制系统

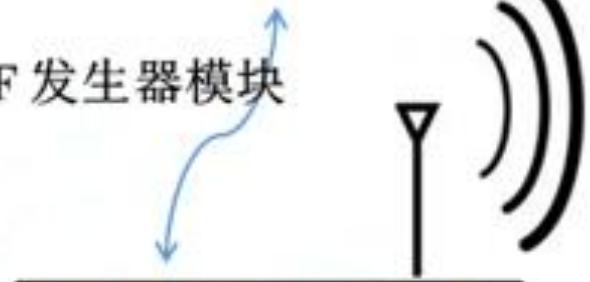
激活条件达成反馈信息

无线远端命令控制

解调处理模块

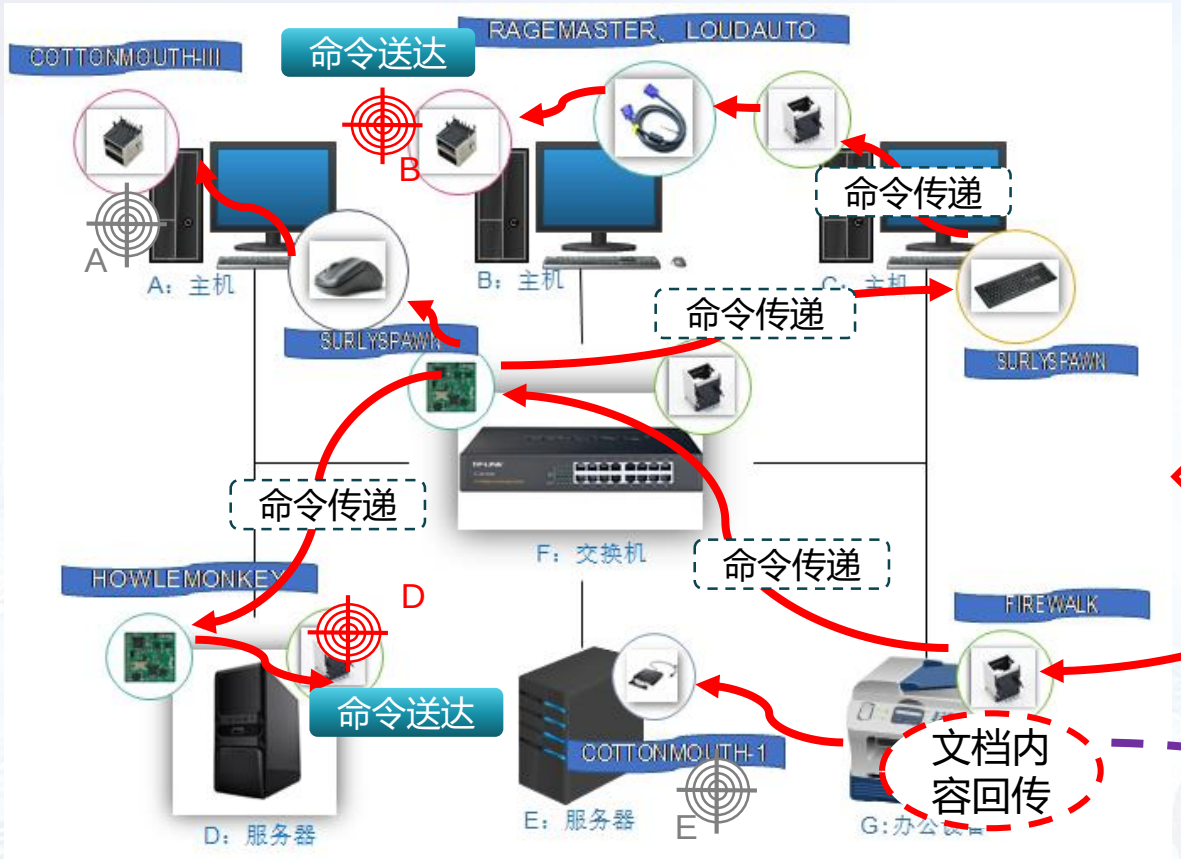
NIGHTWATCH

RF 发生器模块



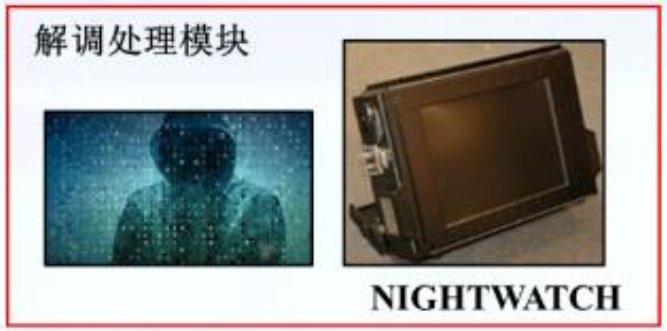
CTX4000/
PHOTOANGLO

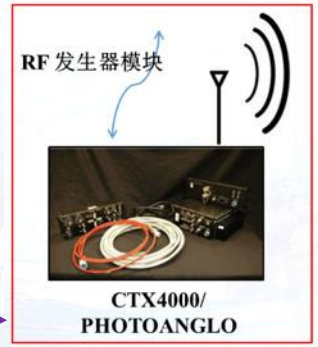
虚拟场景全过程推演——控制



远程启动

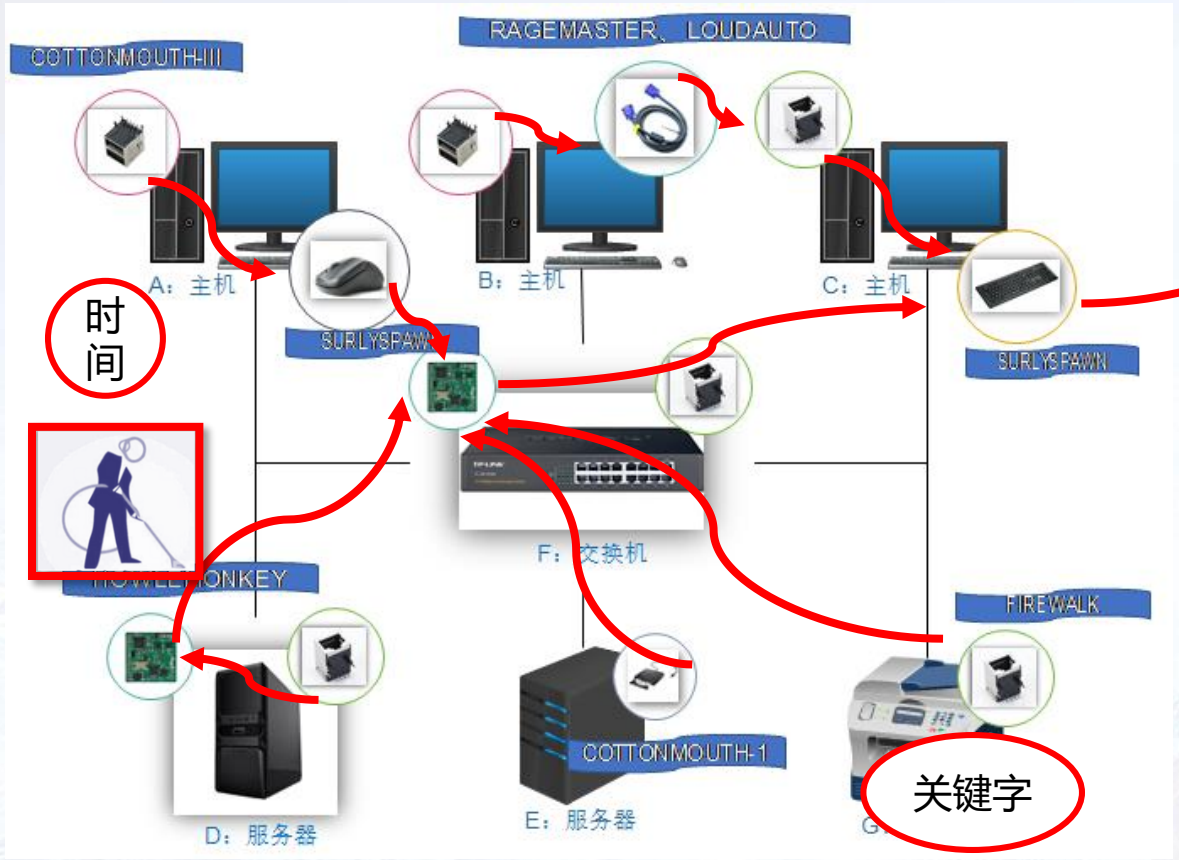
远程启动控制命令下达

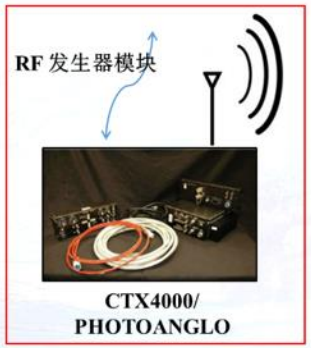




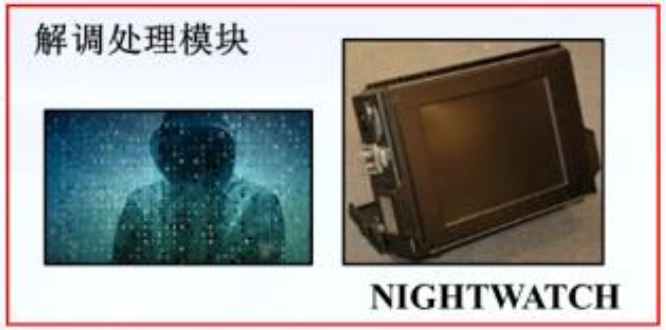
远程控制系统

虚拟场景全过程推演——反馈





远程控制系统



1.主机信息　2.网络数据
3.打印文档　4.屏幕内容

网空威胁之硬件威胁推演——攻击总结

- **核心突破以人和硬件装备为主**
  - 外部和内部人员
  - 专用硬件装备
- **硬件攻击威胁覆盖大部分办公设备**
  - 计算机
  - 服务器
  - 交换机
  - 显示器
  - 键盘
  - 鼠标
- **常规软件检测手段无法有效发现威胁**
  - 部分装备基于更底层手段实现
  - 处于监听模式装备基本无法检出
  - 部分装备攻击时可端点、流量等环节有所发现
- **功能强大，某些方面远超常规网络攻击能力**
  - 重要数据信息
    - 主机
    - 网络
    - 显示
    - ……
  - 恶意载荷
  - 控制命令
- **不依赖现有网络传输数据**
  - 短距离网状网络数据传输
  - 长距离级联网络数据传输
- **可对目标造成物理性损坏**
  - 主机破坏
  - 网络破坏

网空威胁之硬件威胁推演——防御方案

- **物理隔离网络并不可靠**
  - 人
  - 物流
  - 供应链
  - 仓储
  - 硬件装备
- **单点防御无法解决这种威胁**
  - 威胁涉及面广
  - 无法有效检测所有威胁
  - 持续的单威胁装备产生

防御方案

- **物理安全、人员安全和供应链路安全相结合的多维度综合防御体系，最大限度的降低被突破的可能性**
- **通过整体的网络综合防御体系解决被突破后，及时发现威胁、定位威胁和解决威胁的能力，有效防御网络可能遭受的多种威胁。**

网络空间威胁对抗与态势感知研讨会
暨 第六届安天网络安全冬训营

THANKS

扫码关注冬训营动态

战术型态势感知指控积极防御
协同响应猎杀威胁运行实战化

铁流鏖戰