APT攻击技术学习指南 v1.0 （S.R.P 2019-2-14）

目标侦察 → 木马制作 → 木马投递 → 控制&渗透 → 数据回传

S.R.P

Idear&bug提交

当前版本：v1.0 不定期更新

项目启动

目标侦察

- **信息收集**
  - 技术信息收集
    - 域名、ip空间确定
    - 网站、博客、业务地址收集
    - 网络拓扑、业务架构收集
    - OSINT公开技术数据收集
    - 供应链技术信息收集
  - 人员信息收集
    - 邮箱、用户名、社交账号收集
    - 职务、组织角色、人物关系收集
    - 社保、家庭成员、家庭住址、债务情况收集
    - 第三方人员信息收集
  - 组织信息收集
    - OSINT组织公开信息收集
    - 法人、股东结构、组织架构收集
    - 组织公开业务、产品文档收集
    - 组织物理位置、办公场所信息收集
    - 第三方供应商合作业务识别
- **弱点识别**
  - 技术弱点识别
    - 应用漏洞识别
    - 网络及配置安全分析
    - 安全防御能力分析
    - 第三方库、组件漏洞识别
  - 人员弱点识别
    - 分析人员组织架构从属关系分析
    - 分析组织内部社交关系
  - 组织弱点识别
    - 组织业务流弱点识别
    - 组织管理及职能部门弱点识别
    - 组织物理安全分析
    - 第三方供应商及外包安全

木马制作

- **木马选择**
  - PC远控
    - win平台：Cobalt Strike、NJRAT、Remcos CHAos-RAT、gh0st、QuasarRAT、Revenge RAT
    - ios平台：EvilOSX、JRAT、Pupy
    - linux平台：JRAT、Pupy
  - 移动端远控
    - 安卓：AhMyth、DroidJack、SpyNote
    - 苹果：Eggshell
  - 其他远控：Galileo RCS
- **木马伪装**
  - Office（DDE、OLE、公式编辑器、EPS、VBA、其他）、Flash、hta、pdf、CHM文件嵌入马
  - lnk马快捷方式伪装
  - RLO文件名伪装
  - 自解压马
  - PE捆绑
  - 后缀隐藏
    - 图片：FakeImage..
    - PPT：backdoorppt
    - 其他：exe图标资源修改器Resource Hacker
- **木马免杀**
  - 捆绑：backdoor-factory、pyJoiner、Shellter
  - AVET、Veil免杀
  - 数字签名伪造：SigThief、signtools、Digital-Signature-Hijack
  - APK混淆：AVPass
- **C2命令控制器组建**
  - C2服务器ip发布
    - 利用域名发布C2服务器ip
    - 利用合法网站发布C2服务器列表
  - 域名注册
    - 高信誉过期域名抢注：expireddomains.net
    - DGA伪随机域名注册
    - 拉丁字母相似域名注册：EvilURL
  - 命令控制器
    - 自建私有控制器
      - 控制器ip隐藏
        - 分布式IP重定向
        - Tor Fronting
        - Domain Fronting域前置
        - CDN+https+websocket
        - Apache mod_rewrite HTTP重定向
      - 流量混淆：Malleable C2、ExternalC2
      - 后备通道
    - 利用合法网站/api建立控制器
      - 利用twitter、github、Gmail、Dropbox发送接受命令
      - 利用社交聊天API发送接收命令执行结果
  - 控制器内网上线：ngrok、FRP、XTunnel、N2n

木马投递

- **鱼叉攻击（邮件）**
  - 投递文案策划
    - 目标喜好分析
    - 目标近期活动分析
    - 钓鱼文案编写
  - 邮件html模板制作
  - 发件人地址伪装
    - 同服邮箱账号注册
    - 相似域名注册：EvilURL
    - 发件人伪造：swaks、代发api
  - 邮件安全网关绕过
    - 防欺骗能力检测：SpoofCheck
    - 钓鱼连接检测绕过：白名单域名URL跳转漏洞
    - 发送频率控制
    - 高信誉邮件代发服务
  - 钓鱼邮件批量投递管理系统：FiercePhish、Gophish、king-phisher
- **现场投递**
  - 无线网络攻击
    - 无线密码破解：NetHunter、万能钥匙
    - 流量劫持注入：BDFProxy
  - Badusb HID攻击
    - 硬件选择：ps2303芯片U盘、树莓派zero w、Teensy开发板、其他
    - 固件程序：P4wnP1、Psychson、USB-Rubber-Ducky、360GhostTunnel
  - 存储介质攻击：感染木马文件的光盘、U盘、移动硬盘
  - 物理入侵：ID卡伪造、门禁破解、角色扮演、身份伪装
- **水坑攻击**
  - 常用网站挂马
    - 行业、组织网站挂马：网站、论坛、博客
  - 开放目录挂马
    - 行业、组织开放目录挂马：网盘、共享目录
  - 浏览器攻击框架
    - Beef
    - Browsersploit
- **供应链攻击**
  - 通用软件供应链攻击
    - 软件下载/更新源劫持
      - 安装源攻击：pip/apt-get源劫持
      - 破解、汉化软件后门
        - 开发工具后门：案例xcodeGhost
        - 运维工具后门：案例XshellGhost、putty
      - 刷票、翻墙、视频播放工具后门
    - 基础设施后门利用
      - 网络设备后门
      - 物联网iot设备后门
  - 软件外包商攻击
    - 源代码攻击（svn、补丁服务器）
    - 第三方调用资源攻击（组件库、js库、js广告代码）

控制&渗透

- **特权维持：**权限维持后门植入
- **横向渗透**
  - 口令/凭证收集
    - Mimikatz
    - LaZagne
  - 域渗透：PowerTools工具集
  - NSA方程式1day漏洞利用
  - WEB应用及组件REC漏洞利用
  - 弱口令攻击
  - 数据库渗透：未授权、弱口令
  - 权限提升：kernel-exploit、Exploit Suggester
- **蛙跳攻击**
  - 安全域绕过
    - 防火墙绕过
    - 堡垒机绕过
  - 网络跳板：netsh、lcx、nc、ew、ssocks、Termite、reGeorg、Tunna
- **摆渡攻击**
  - USB木马中继
    - 识别员工USB写入木马
    - 搜集机密文件文件写入USB隐藏分区
    - 联网回传
  - WHID攻击中继：自带wifi模块或上网卡的HID设备
  - 无人机攻击中继

数据回传

- **数据采集**
  - 音、视频捕获集
  - 屏幕捕获
  - 键盘记录
  - USN硬盘文件列表收集
  - 剪切板读取
  - 电子邮件收集
  - 软件配置文件收集
  - 密码表收集
  - 其他机密文档收集
- **隐蔽传输**
  - 文件回传服务器配置
  - 文件压缩：zip、rar、7z...
  - DLP防泄密绕过：CloakifyFactory
  - 特殊协议隧道：DNSExfiltrator

入门引导

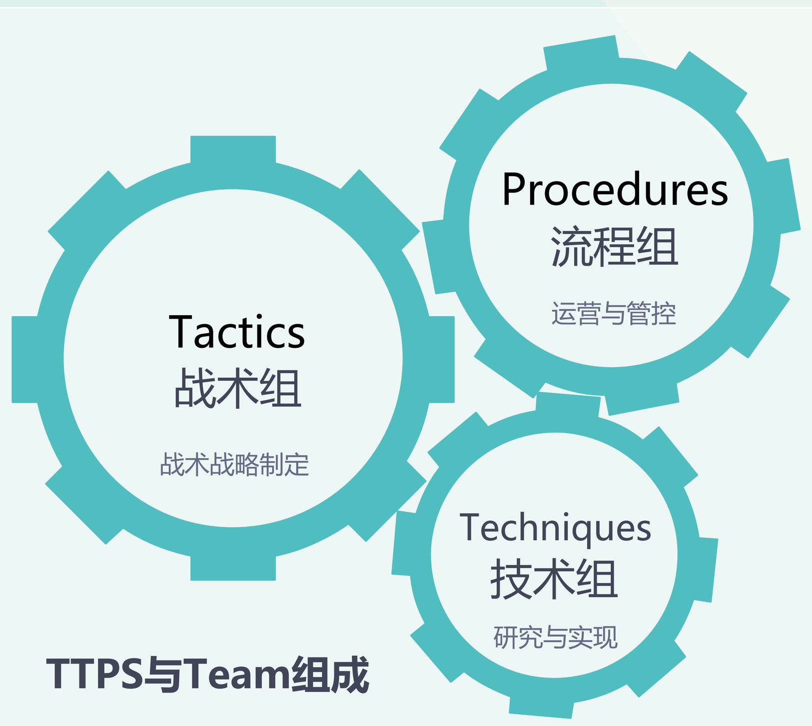
① **知己知彼稳妥出击：**在实战过程中目标 情报收集 的广度决定了APT攻击的深度

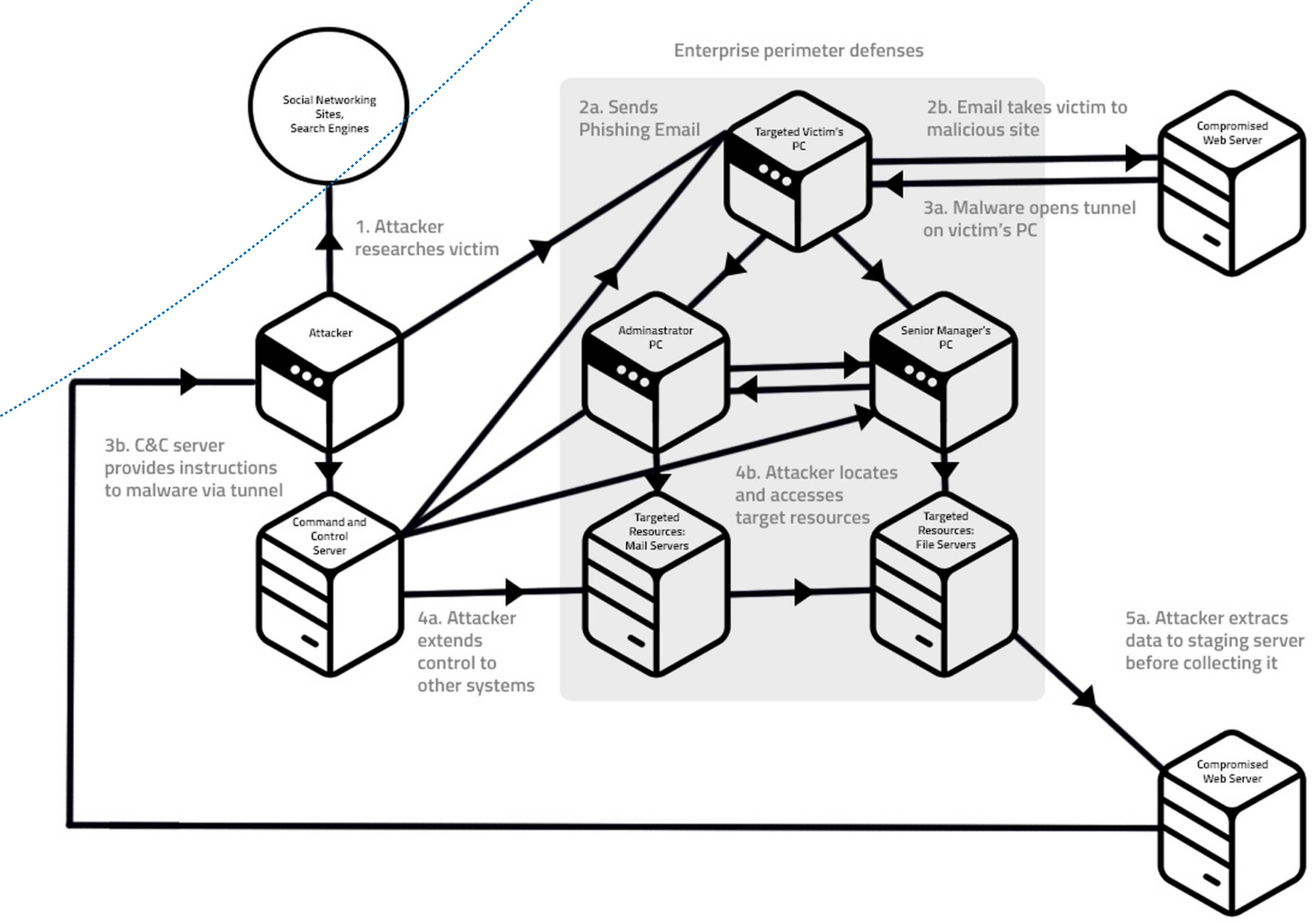
② **上兵伐谋攻心为上：**战术谋略 是决定攻击成败的核心，在APT攻击中，合理利用目标弱点进行欺骗攻击、诱导攻击为上策。

③ **欲善其事先利其器：**工具的好坏取决于使用者的水平。完善 兵器库 ，并通过不断的练习，了解各种工具的实现原理、参数、优劣势和使用场景，才能事半功倍。

④ **兵无常势水无常形：**在实战过程中要根据目标脆弱面和目标环境特点来制定灵活机动的战略战术，不能墨守标准化的作战套路。

⑤ **万物皆虚万事皆允：**行为底线 "每个人都是自身道德、行为的设计者与执行者，每个人都必须承担起因自身的行为所带来的后果，无论是忧伤还是快乐，荣耀或者屈辱。在黑暗中行走，为光明服务。《刺客信条》



TTPS与Team组成

Advanced Persistent Threat Data Extraction