攻防体系之供应链攻击

360Red Team 赖志活

About Me

- 赖志活，Wfox
- 360Red Team成员
- 从事渗透测试、红蓝对抗、漏洞挖掘、安全研究等方向
- CTF老年选手
- 目前从事CEF浏览器框架安全研究，曾发现QQ、TIM、微信的RCE漏洞

1. 供应链的起源与趋势

初识供应链安全

供应链的威胁来源

2. 供应链面临的攻击面

web站点供应链攻击样例

实战中网络攻击面临的攻击面

供应链攻击案例

企业引入供应链引发的风险

3. 如何应对供应链上的威胁

供应链安全体系建设

建立可回溯的资产管理体系

企业防范措施

应对案例

供应链的起源与趋势

供应链安全

供应链：从开发到将产品由供应商交付给客户所涉及的组织、人员和系统等。

供应链攻击：通过攻击第三方供应商的软件、硬件、代码、系统等目标达到控制目标企业系统权限的目的。

为什么讲供应链安全

2017年：供应链攻击的引爆点

美国国家反情报与安全中心宣布，2017年是供应链网络攻击的“分水岭”。自上一年以来，供应链网络攻击增长了400%。这仅仅是已知的事件，未记录的事件预计还有更多。

发生最严重的供应链攻击，影响全球范围的WannaCry勒索病毒攻击，影响IT、能源、制造、医疗、电信和运输等行业。

2018年：供应链攻击激增

从2018年5月到2018年9月，平均每月有7次网络攻击。最突出的事件之一是中远船务于2018年7月24日停运，攻击导致了供应商、船只、客户、码头直接的通讯瘫痪。

via DHL Resilience360

供应链安全趋势

攻击趋势上升

供应链攻击事件越演越烈，经济利益、数据窃取等行为从未止息。

起步晚

在近年来才重点开展供应链安全的研究和体系推进工作。

体系标准建设

中科院、多家领头公司参与制订ICT供应链安全标准。

供应链攻击特点

影响范围广

处于供应链上游，一旦遭受攻击，波及下游供应链节点。

攻击面广

供应链中引入的环节越多，攻击面就越广，风险越大。

隐蔽能力强

- 默认信任心理
- 后门模块免杀
- 官方数字签名

检测成本高

涉及环节太多，每个环节接入审查，耗时耗力。

供应链攻击案例

01

Xcode

污染非官方渠道下载的苹果Xcode开发工具，向Xcode编译的APP中植入恶意代码。

02

Xshell

终端模拟软件Xshell的关键模块被植入了恶意代码。

03

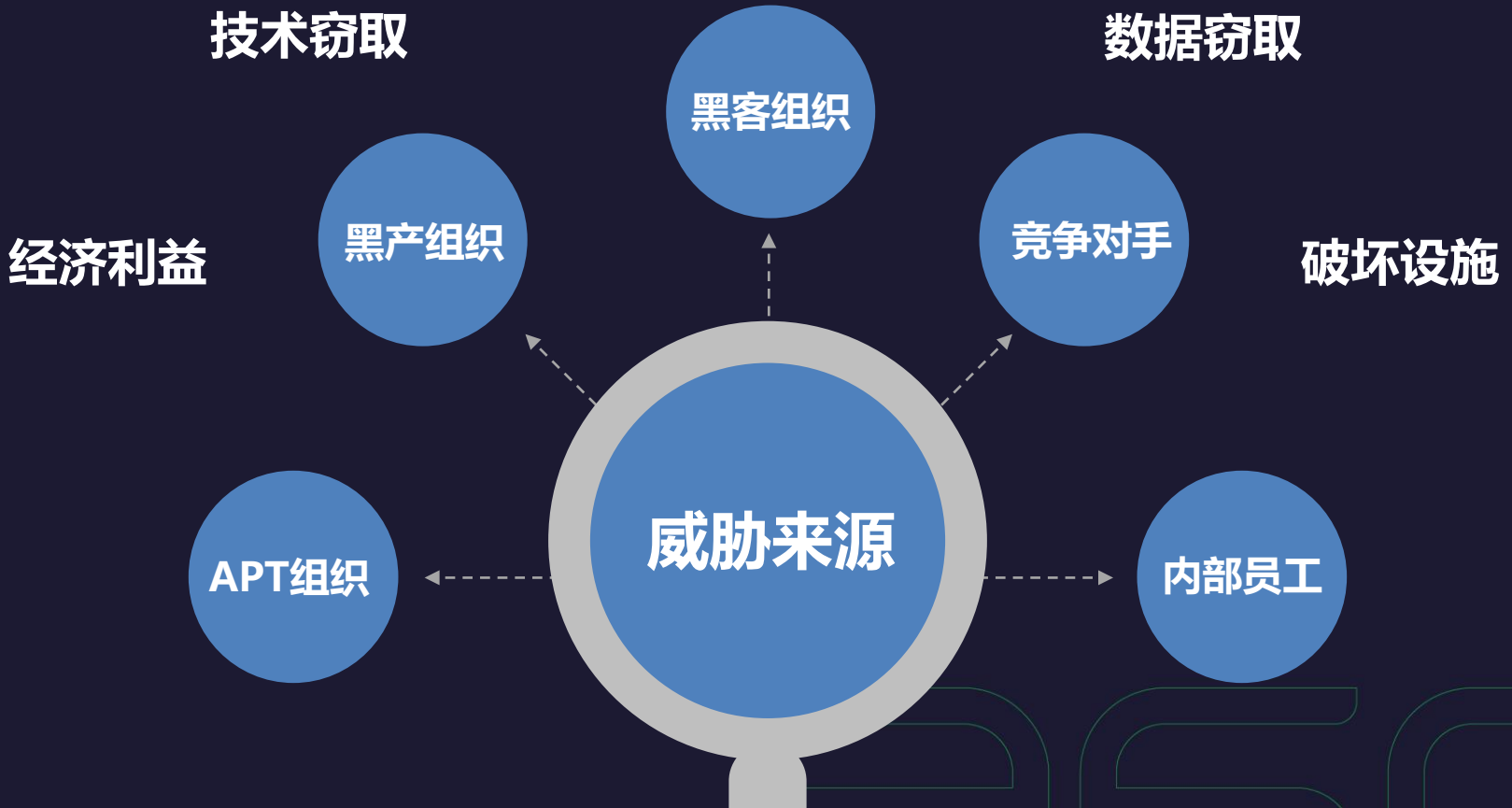
驱动人生

软件升级服务器被控制，下发恶意程序，被控制之后还会感染内网机器进行挖矿。

04

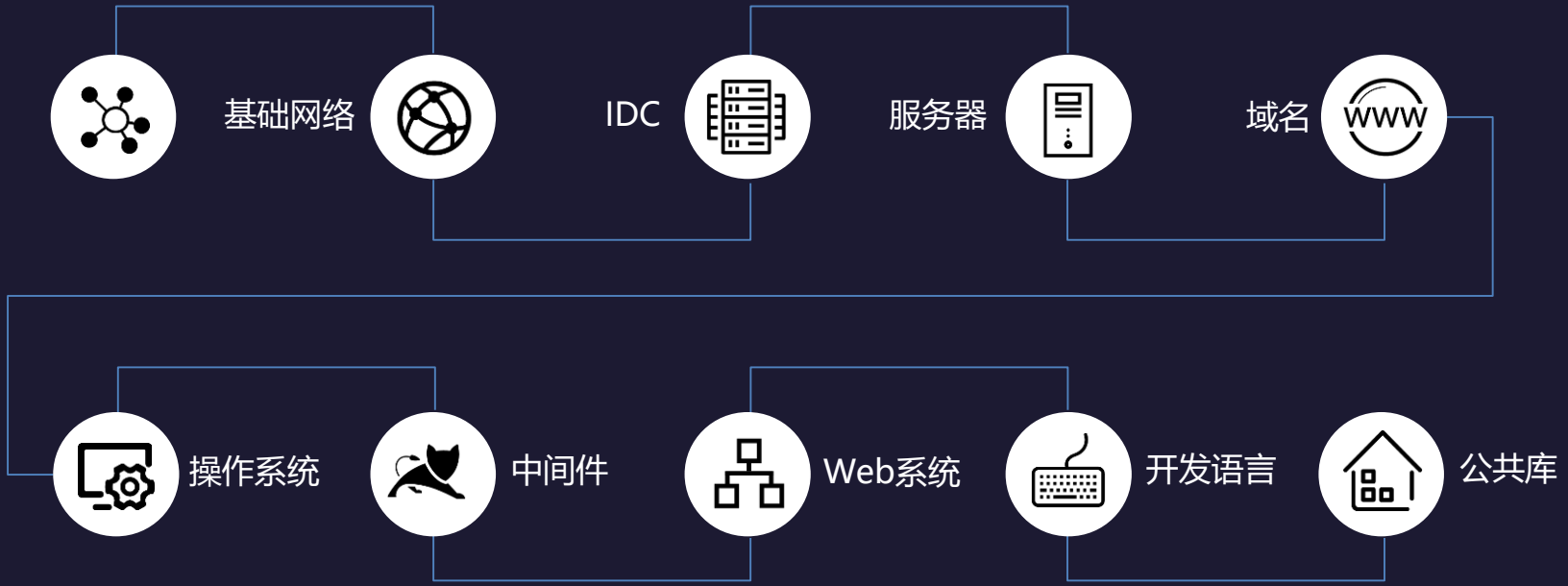
PhpStudy

PHP环境软件phpStudy官方安装包遭篡改，植入了后门代码。

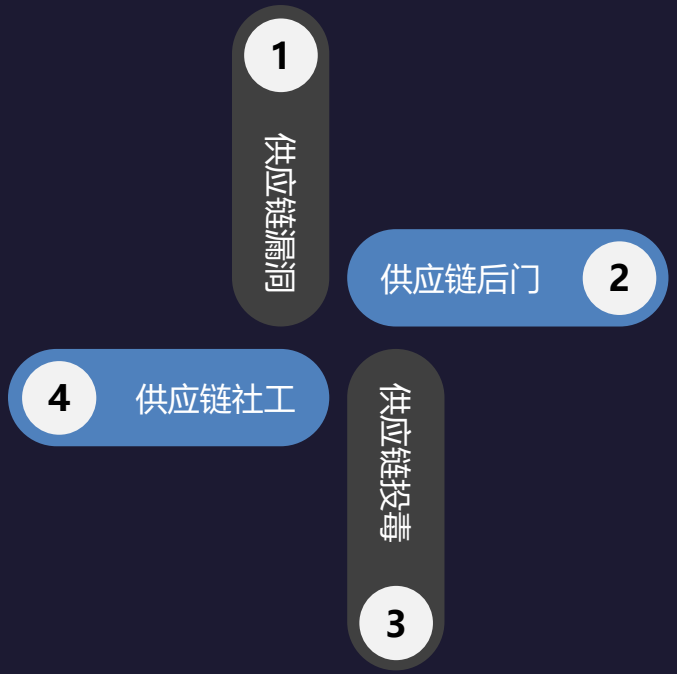

技术窃取
数据窃取
黑客组织
经济利益
黑产组织
竞争对手
破坏设施
威胁来源
APT组织
内部员工

供应链面临的攻击面

供应链样例



寻找攻击点



供应链漏洞

位于供应链下游，最直接有效的攻击手法，利用0day、Nday及其他漏洞突破边界。

供应链后门

预留调试后门、内置口令等，常常被黑客利用。

供应链污染

无差别攻击，影响范围最广。通常是针对指定人群进行精确打击。

供应链社工

人是最大的安全漏洞，供应链环节越多、所介入的人员角色就越多，涉及的攻击面大大增加。

实战攻击面

互联网侧

DNS

域名

CDN

云服务器

邮服托管

OA

软件开发商

边界侧

防火墙

对外映射服务

VPN

交换机

安全设备

内网侧

交换机

运维管理系统

安全设备

堡垒机

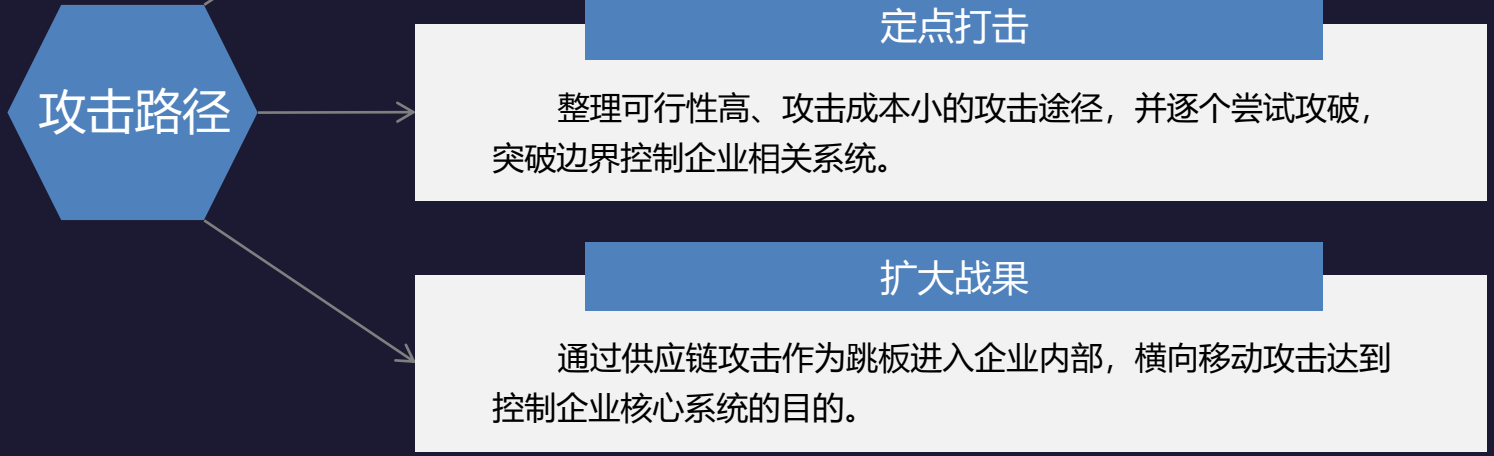
办公侧

钓鱼

终端管理系统

办公软件

BadUSB


攻击路径
信息收集
从供应链层面进行收集，整理出可能存在的攻击点。如母公司、子公司、第三方服务商、第三方产品。
定点打击
整理可行性高、攻击成本小的攻击途径，并逐个尝试攻破，突破边界控制企业相关系统。
扩大战果
通过供应链攻击作为跳板进入企业内部，横向移动攻击达到控制企业核心系统的目的。

TeamViewer事件

转发朋友圈

先卸载为妙

只要我够快，黑客他就追不上我

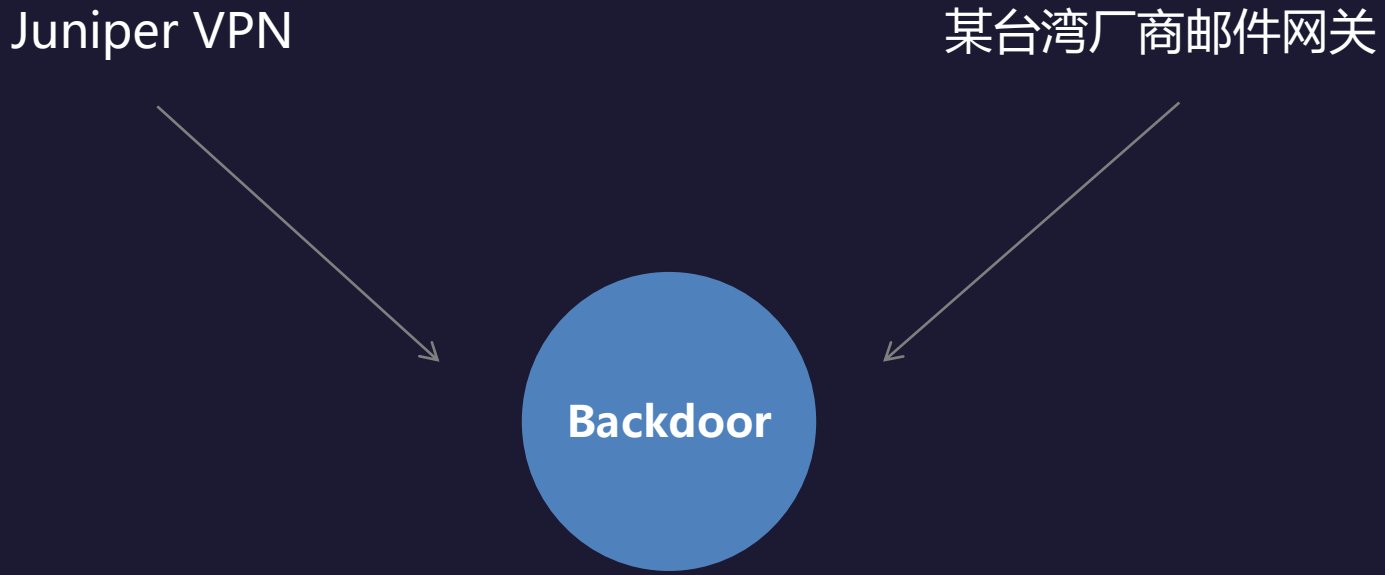
盲目分析

小道消息

历史事件

一次典型的供应链攻击

引入的第三方风险



如何应对供应链上的威胁

供应链安全体系建设

软件供应商

硬件供应商

第三方服务商

建立可回溯的资产管理体系

要全面加强网络安全检查，摸清家底，认清风险，找出漏洞，通报结果，督促整改

资产发现

资产可控

安全运营

防范措施

缩小攻击面

遵循权限最小化原则，收紧企业内网，控制对外映射服务

威胁情报

引入威胁情报，持续监控供应商安全风险

威胁管控

根据互联网侧、边界侧、内网侧、办公侧等场景制定防护方案

案例

中国

- 禁止采购思科路由器、交换机
- 禁止采购迈克菲、赛门铁克、卡巴斯基等安全软件

美国

- 对华为进行技术封锁
- 禁止进口海康威视、大华科技、科大讯飞、旷视科技、商汤科技、依图科技、厦门美亚柏科信息有限公司、颐信科技有限公司等人工智能、人脸识别、大数据信息化、安防监控等厂商

不局限于软件投毒的供应链攻击

更多未知的攻击面

共同努力推动供应链安全发展

THANKS