
FREEBUF
ISC 2015
中国互联网安全大会
360互联网安全中心
ISC
2015
数据驱动安全
2015 中国互联网安全大会
China Internet Security Conference
APT与新威胁论坛

FREEBUF

ISC 2015 中国互联网安全大会

360互联网安全中心

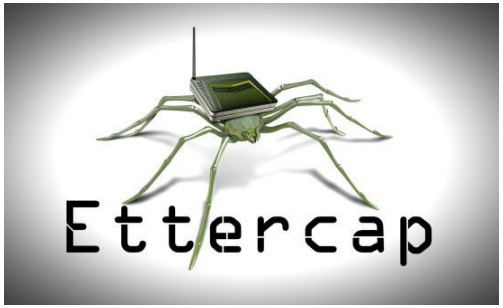
网络安全威胁中的商业秘密

- 从HackingTeam说起
- 商业化间谍软件现状
- 商业军火带来的问题
- 可以采取的应对策略

从]HackingTeam[说起

成立时间	2003年
创始人	David Vincenzetti(CEO) Valeriano Bedeschi(CIO)
核心人物	Alberto Ornaghi(软件架构师) Marco Valleri(进攻安全管理)
总部	米兰，意大利

头像取自领英（Linkedin）

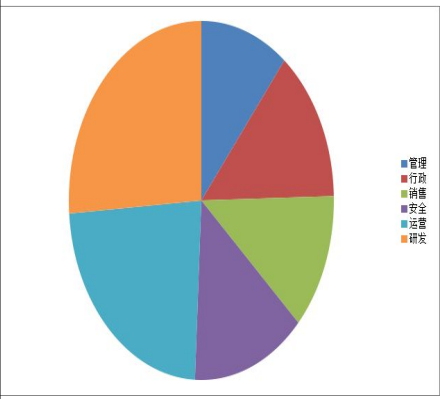


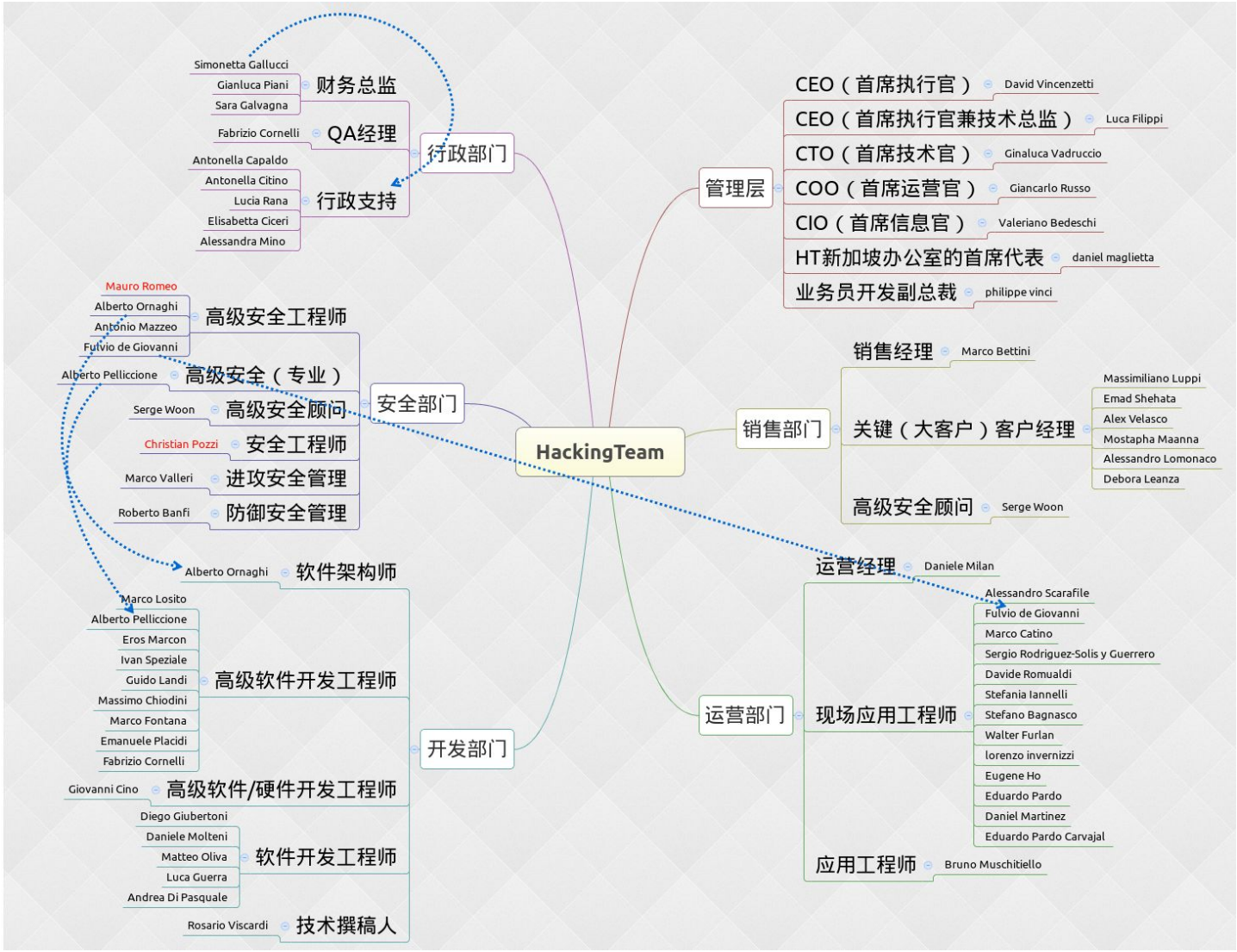
- 免费开源
- 内网安全审计工具
- 基于MITM实现

“第一个面向警方的商用黑客软件”

从]HackingTeam[说起

部门	人数
管理	7
行政	9
销售	8
安全	9
运营	15
研发	17
合计	65





从]HackingTeam[说起

合同额TOP 10 客户

金额单位：EUR

组织名称	国家	区域	最早订单	年费	总收入
PDI	智利	拉美	2014		2,289,155
ISO	乌干达	非洲	2015	831,000	2,197,100
CSDN	摩洛哥	非洲	2009	140,000	1,936,050
	墨西哥	拉美	2010	130,000	1,390,000
DGST	摩洛哥	非洲	2012	160,000	1,237,500
iDA SINGAPORE	新加坡	亚洲	2008	89,000	1,209,967
GID Saudi	沙特阿拉伯	非洲	2012	114,000	1,201,000
UAEIntelligence	阿联酋	非洲	2012	150,000	1,200,000
MOD Saudi	沙特阿拉伯	非洲	2013	220,000	1,108,687
SIS	哈萨克斯坦	欧洲	2012	140,000	1,012,500

从]HackingTeam[说起

主要客户分布

从]HackingTeam[说起

RCS 能力

Windows OSX

BlackBerry Windows Mobile

Android iOS

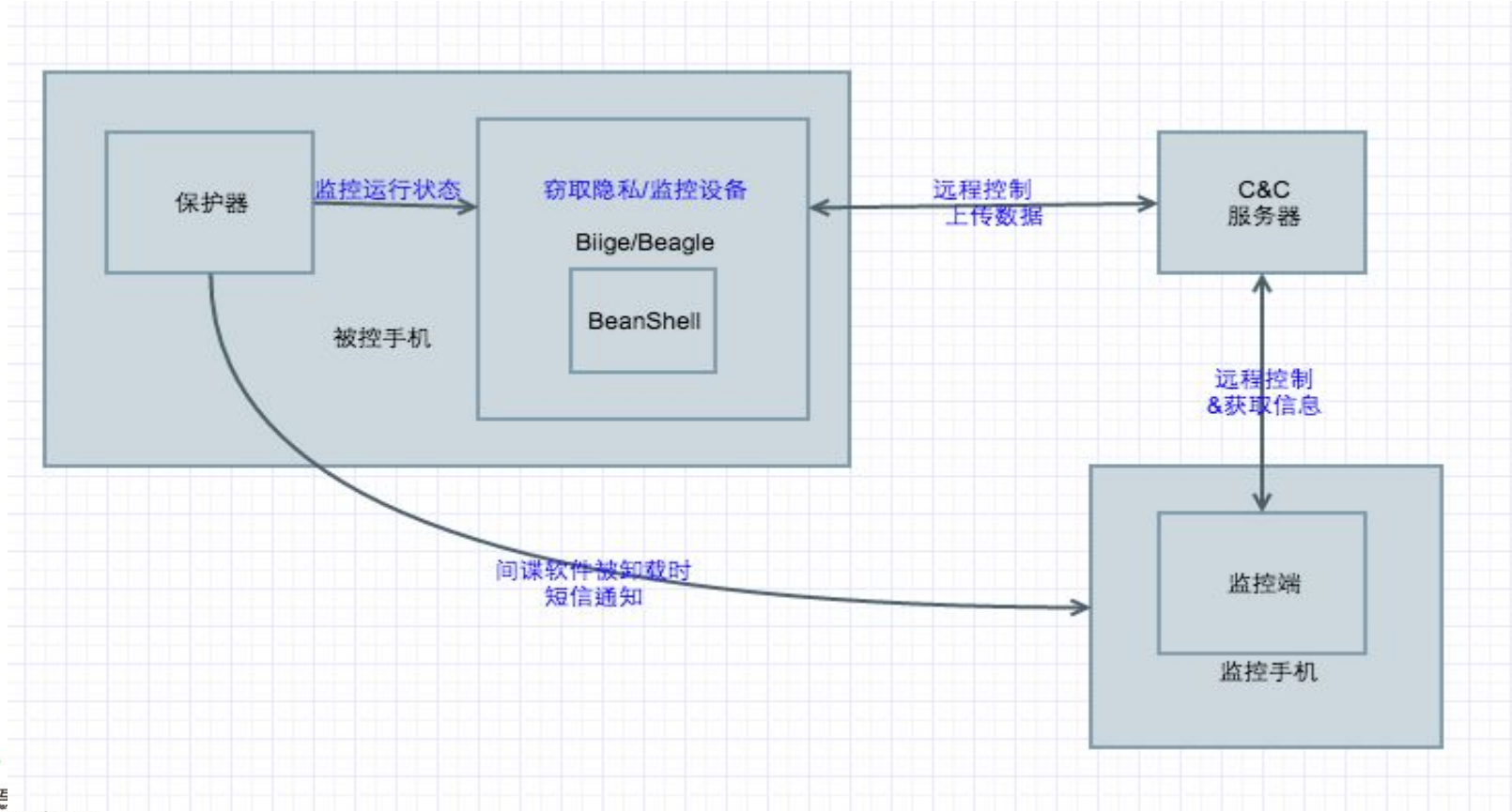
商业化间谍软件现状

- 短信息监控
- Facebook监控
- WhatsApp监控
- LINE监控
- 通话监控
- 位置监控
- 媒体文件监控
- Web访问监控
- 手机开关机记录
- 联系人黑白名单
- 应用程序监控
- 应用黑白名单
- 应用风险状态

商业化间谍软件现状

PhoneBeagle

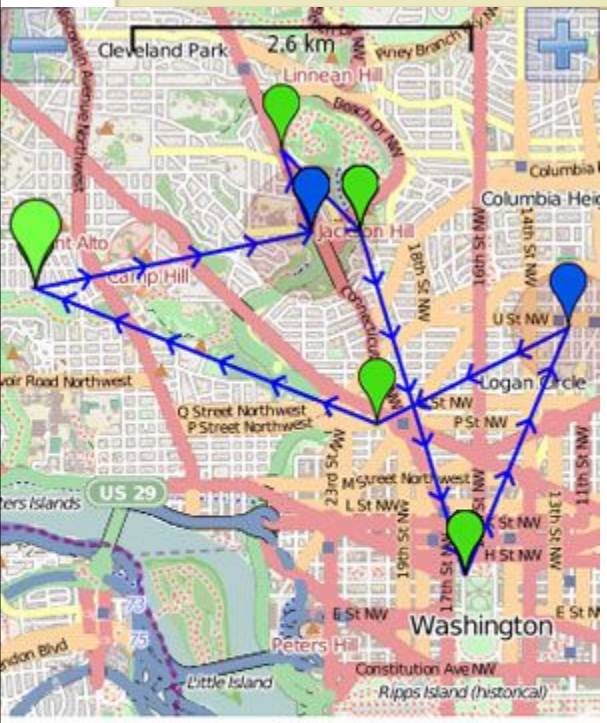
BiiGe 比歌



商业化间谍软件现状

PhoneBeagle

BiiGe 比歌



GPS

Accuracy 10 m **Speed** 0 mph

08/02/2011
14:35:06

08/02/2011

08/02/2011
16:27:52

商业化间谍软件现状

- 多语言界面
- 有/无图标版本（图标可隐藏）
- 安装后在**Services**中可见
- 需要手动激活

- 中文界面
- 安装后无图标
- 安装后在**Services**不可见

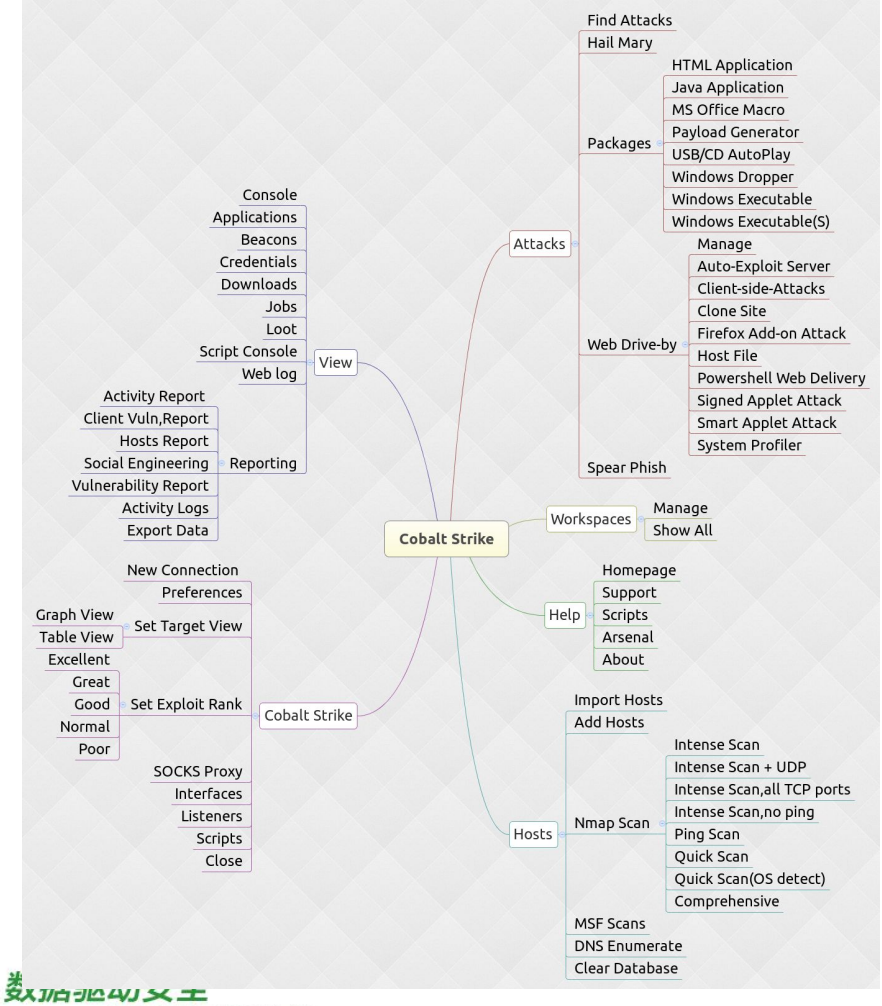
商业化攻击平台
Cobalt Strike

商业化攻击平台
Cobalt Strike

公司/项目/机构	职位	时间
Strategic cyber LLC	创始者和负责人	2012.1-至今
特拉华州空军国民警卫队	领导，传统预备役	2009-至今
Cobalt strike	项目负责人	2011.11-2012.5
TDI	高级安全工程师	2010.8-2011.6
Automattic	代码Wrangler	2009.7-2010.8
Feedback Army, After the Deadline	创始人	2008.7-2009.11
美国空军研究实验室	系统工程师	2006.4-2008.3
美国空军	通信与信息 军官	2004.3-2008-3

姓　　名：Raphael Mudge
教育背景：Syracuse University 美国雪城大学；密歇根科技大学
目前就职：Strategic Cyber LLC（战略网络有限责任公司）；特拉华州空军国民警卫队

商业化攻击平台
Cobalt Strike



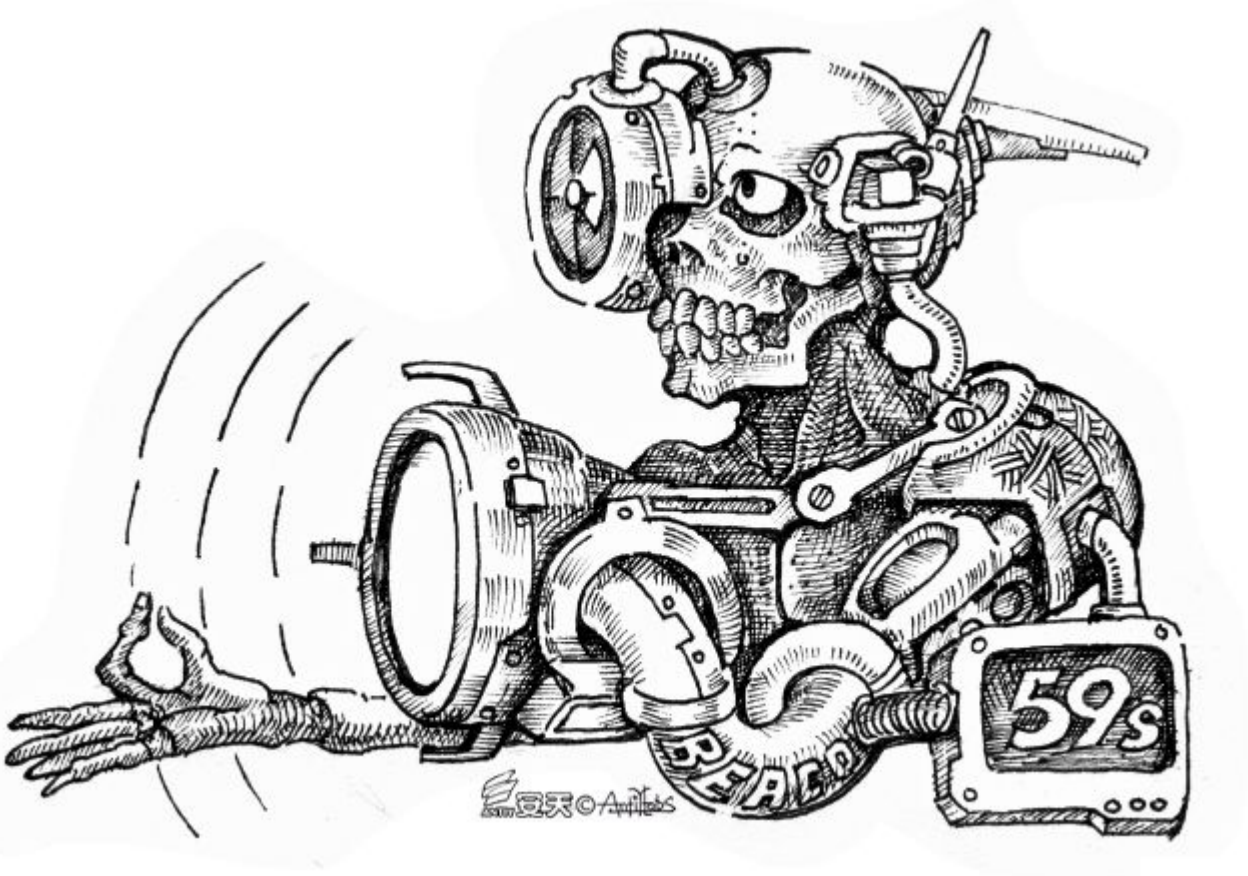
Packages

- HTML Application
- Java Application
- MS Office Macro
- Payload Generator
- USB/CD AutoPlay
- Windows Dropper
- Windows Executable
- Windows Executable(S)

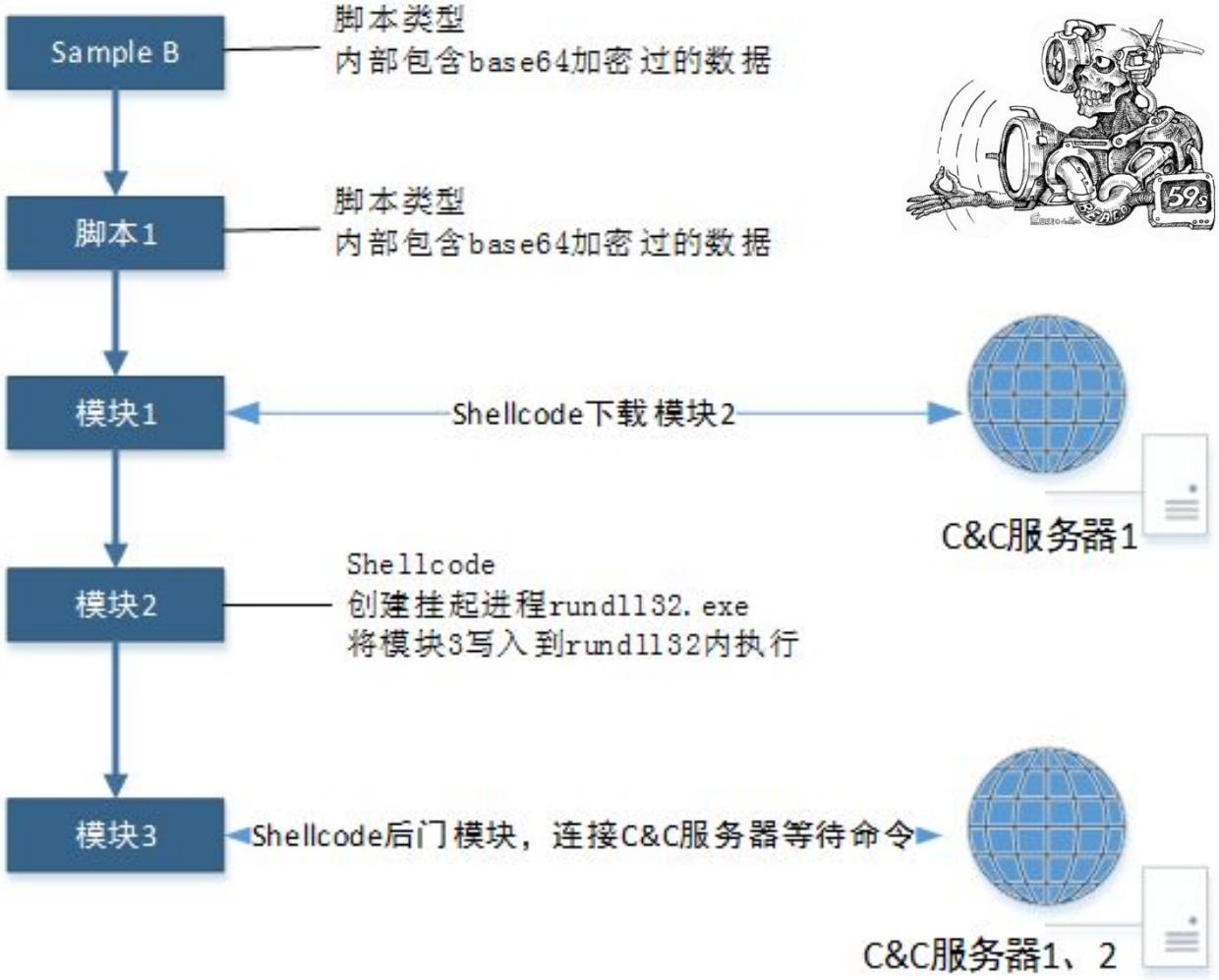
Web Drive-by

- Manage
- Auto-Exploit Server
- Client-side-Attacks
- Clone Site
- Firefox Add-on Attack
- ……

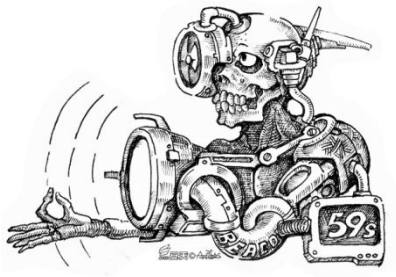
真实案例
APT TOCS



真实案例
APT TOCS



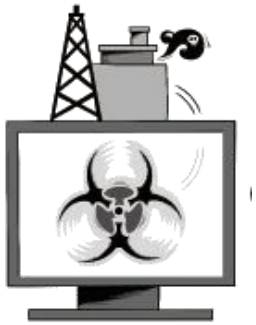
真实案例
APT TOCS



商业军火带来的问题

我们面对怎样的对手

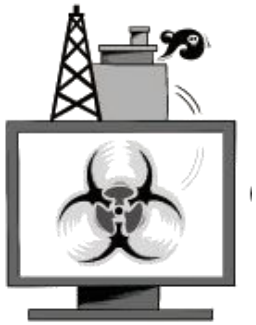
“超级病毒”、“超级工厂病毒”、“超级武器”、“潘多拉的魔盒”



利用了微软操作系统中至少4个漏洞，其中有3个全新的零日漏洞；为衍生的驱动程序使用有效的数字签名；通过一套完整的入侵和传播流程，突破工业专用局域网的物理限制；利用WinCC系统的2个漏洞，对其开展破坏性攻击。它是第一个直接破坏现实世界中工业基础设施的恶意代码。据赛门铁克公司的统计，目前全球已有约45000个网络被该蠕虫感染，其中60%的受害主机位于伊朗境内。伊朗政府已经确认该国的布什尔核电站遭到Stuxnet蠕虫的攻击。

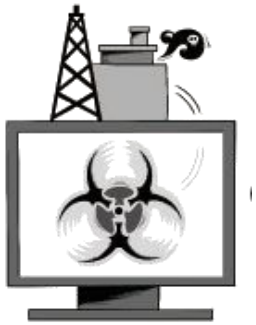
商业军火带来的问题

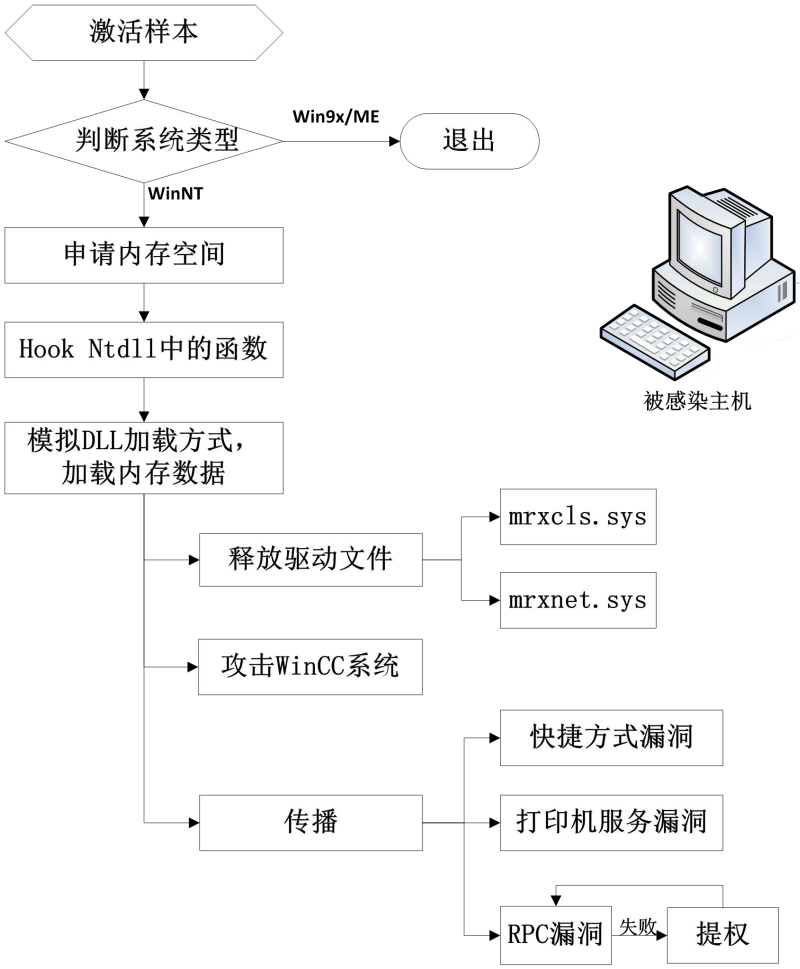
我们面对怎样的对手

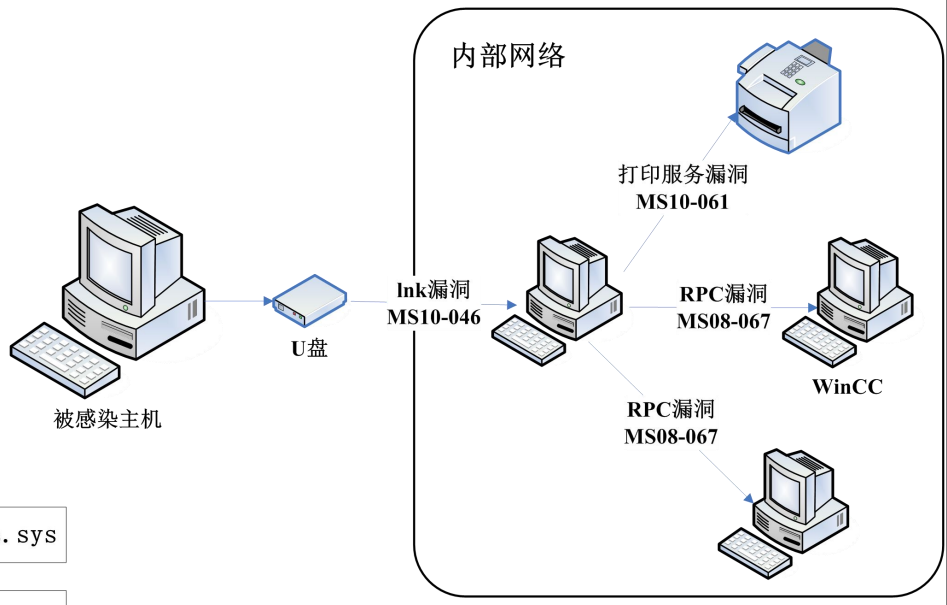


商业军火带来的问题

我们面对怎样的对手



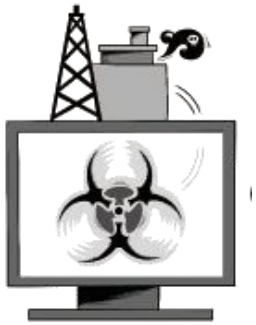




商业军火带来的问题

我们面对怎样的对手

视频演示



商业军火带来的问题

我们面对怎样的对手

2012年5月，俄罗斯安全专家发现一种威力强大的电脑病毒“火焰”(Flame)在中东地区大范围传播。俄罗斯电脑病毒防控机构卡巴斯基称，这种新病毒可能是“某个国家专门开发的网络战武器”。

“火焰”病毒最早可能于2010年3月就被攻击者放出，但一直没能被其他网络安全公司发现。主要感染中东地区。它由一个20MB大小的模块包组成，共包含20个模块且每个模块有着不同的作用。flame的体积十分庞大并且结构极为复杂，被称为有史以来最复杂的病毒，因此很难追踪它的感染途径。受害者的范围极其广泛，从个人到国家机构及学术和教育体系等。

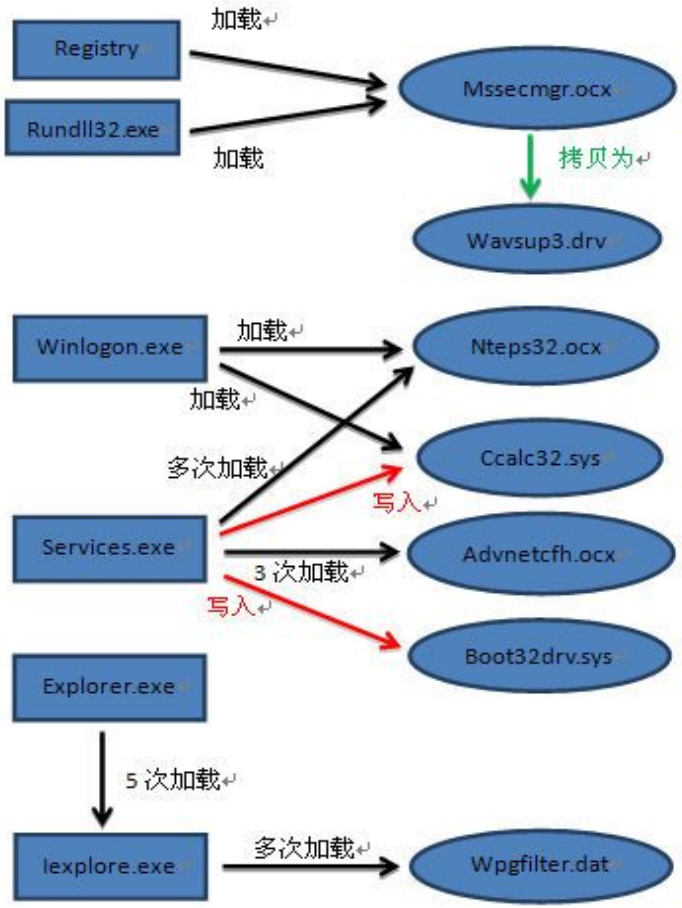
Flame病毒可以通过USB存储器以及网络复制和传播，并能接受来自世界各地多个服务器的指令。感染“火焰”病毒的电脑将自动分析自己的网络流量规律，自动录音，记录用户密码和键盘敲击规律，并将结果和其他重要文件发送给远程操控病毒的服务器。一旦完成搜集数据任务，这些病毒还可自行毁灭，不留踪迹。

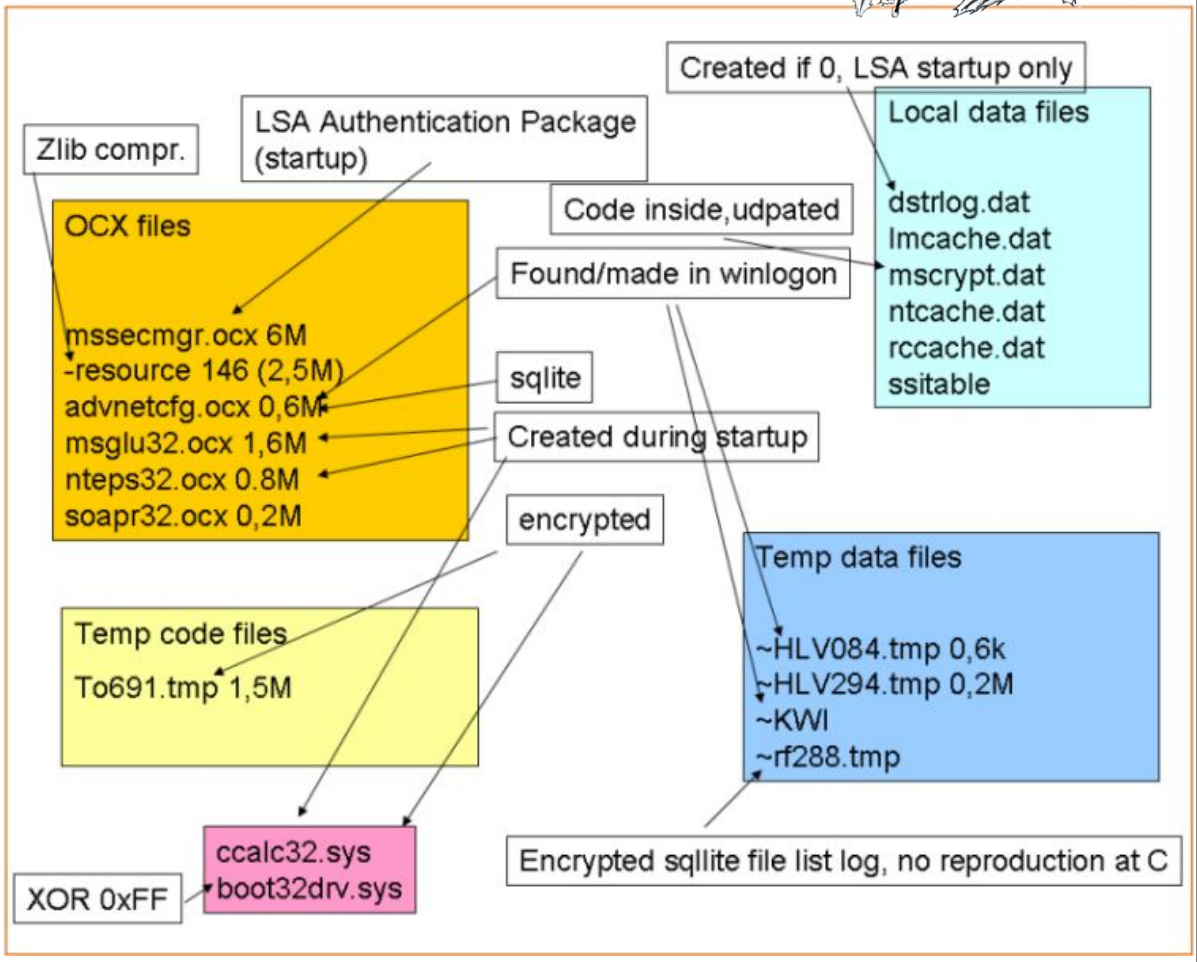
商业军火带来的问题

我们面对怎样的对手

商业军火带来的问题

我们面对怎样的对手



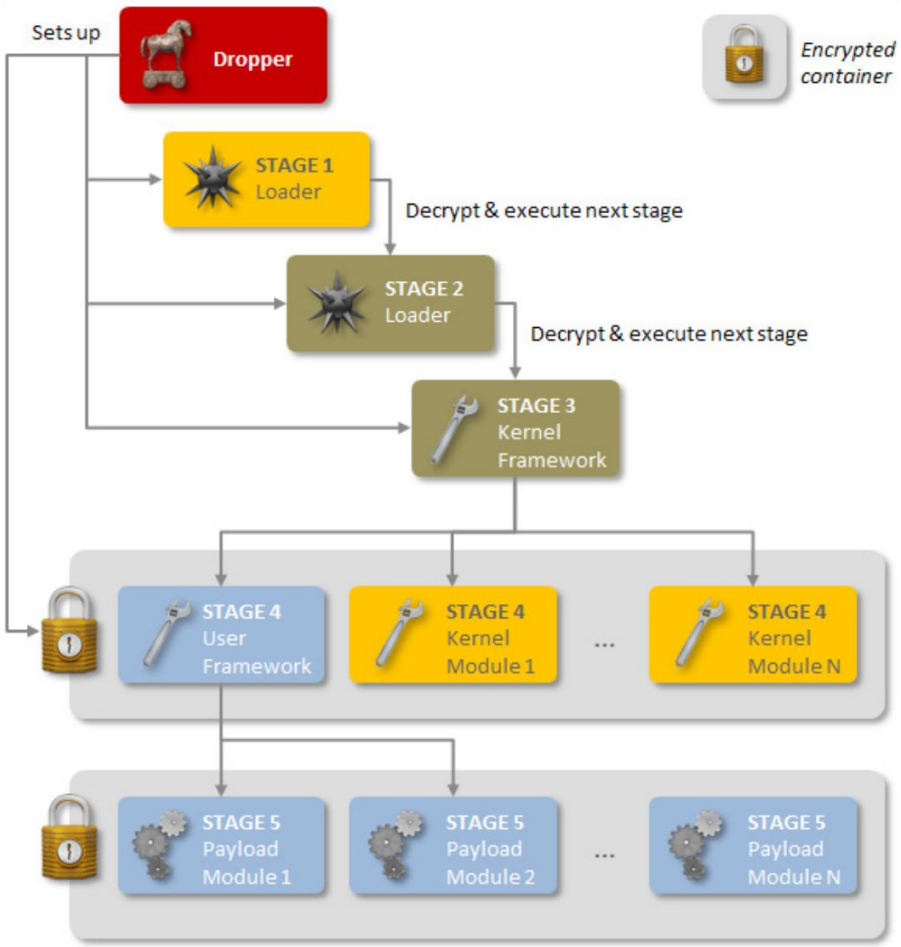


商业军火带来的问题

我们面对怎样的对手

商业军火带来的问题

我们面对怎样的对手



Regin的六个阶段	
阶段	组件
阶段 0	投放器。安装Regin 至目标计算机
阶段 1	加载驱动程序，唯一明显可见的代码，其余各阶段均加密数据形式存储
阶段 2	加载驱动程序
阶段 3	加载压缩、解密、联网及处理加密的EVFS程序
阶段 4	利用EVFS并加载额外的内核模式驱动程序，包括有效载荷。
阶段 5	主要的有效载荷和数据文件

商业军火带来的问题

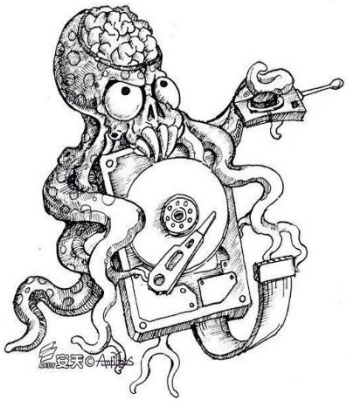
我们面对怎样的对手

部分功能插件功能

文件类型	编号	描述
SYS	0003	驱动程序
SYS	C433	Rootkit
SYS	C42B	PE加载程序
SYS	C42D	DLL注入
SYS	C3C3	类似WinPcap的网络数据包过滤器驱动程序（协议过滤器版本3.5） 用于设置TCP和UDP穿透过滤器和绕过防火墙。 执行BPF（Berkeley包过滤器）字节码，存储在阶段5的数据文件里。
SYS	CE69	网络端口屏蔽器
DLL	C363	网络数据包捕获
DLL	4E3B	通过注册表或配置文件（如prefs.js, refs.js等）检索网页浏览器（IE浏览器，网景，火狐等）的代理信息。枚举会话和用户账户。
DLL	290B	密码窃取器： • Windows资源管理器凭据 • Windows资源管理器受保护存储记录 • IE合法设置 • 名为“cryptpp”登陆通知数据包的数据
DLL	C375	C&C HTTP/cookies
DLL	C383	SSL通信
DLL	C361	支持加密功能
DLL	001B	ICMP反向信道
DLL	C399	ApplicationLog.Evt记录创建程序
DLL	C39F	进程文件：%Temp%\~b3y7f.tmp
DLL	C36B	UI manipulation • 截屏 • 记录键盘操作 • 锁定工作站/输入Ctrl-Alt-Del • 点击功能 (通过三条指令：去、点击并释放、返回原始位置) • 结束进程
DLL	C351	文件系统探索元和包括原始NTFS解析器的取证水平探索： • 获取其他文件信息和属性 • 浏览记录 • 读写文件 • 移动和复制文件 • 读取并修复部分或全部被删除的文件 • 计算文件哈希
DLL	2B5D	进程和模块操作： • 读取进程和模块 • 进程运行的时间、限制和权限 • 扫描时，跳过俄语或英语的微软文件 • 检测过去两天里新引进的PE文件
DLL	C3CD	枚举 %System%\CurrentControlSet\Services\Tcpip\Linkage\bind里的TCP/IP接口
DLL	C38F	TCPDump 功能
DLL	C3C5	Libnet 二进制文件
DLL	27E9	IIS 网页浏览器日志窃取 通过COM对象枚举发现IIS日志。检索部分或全部日志信息。 • 部分：日志类型、上一个日志、较早日志的时间戳 • 全部：被发掘的全部日志记录

商业军火带来的问题

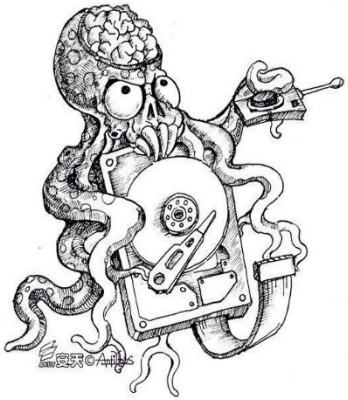
我们面对怎样的对手



- 卡巴斯基安全实验室在**2015**年**2**月**16**日起发布系列报告披露了一个“可能是目前世界上存在的最复杂的网络攻击组织”——“方程式”组织（**Equation Group**）。据卡巴斯基实验室称，该组织使用的**C&C**早在**1996**年就被注册，这暗示了该组织可能已经活跃了**20**年之久。多年以来，他们因总能比其他组织早发现漏洞，从而具有绝对的优势。

商业军火带来的问题

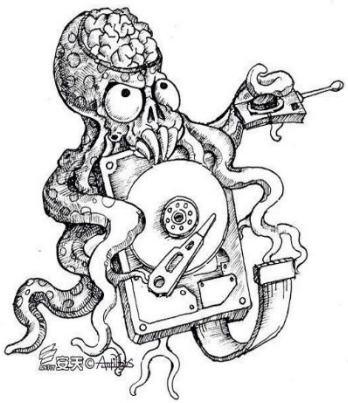
我们面对怎样的对手



商业军火带来的问题

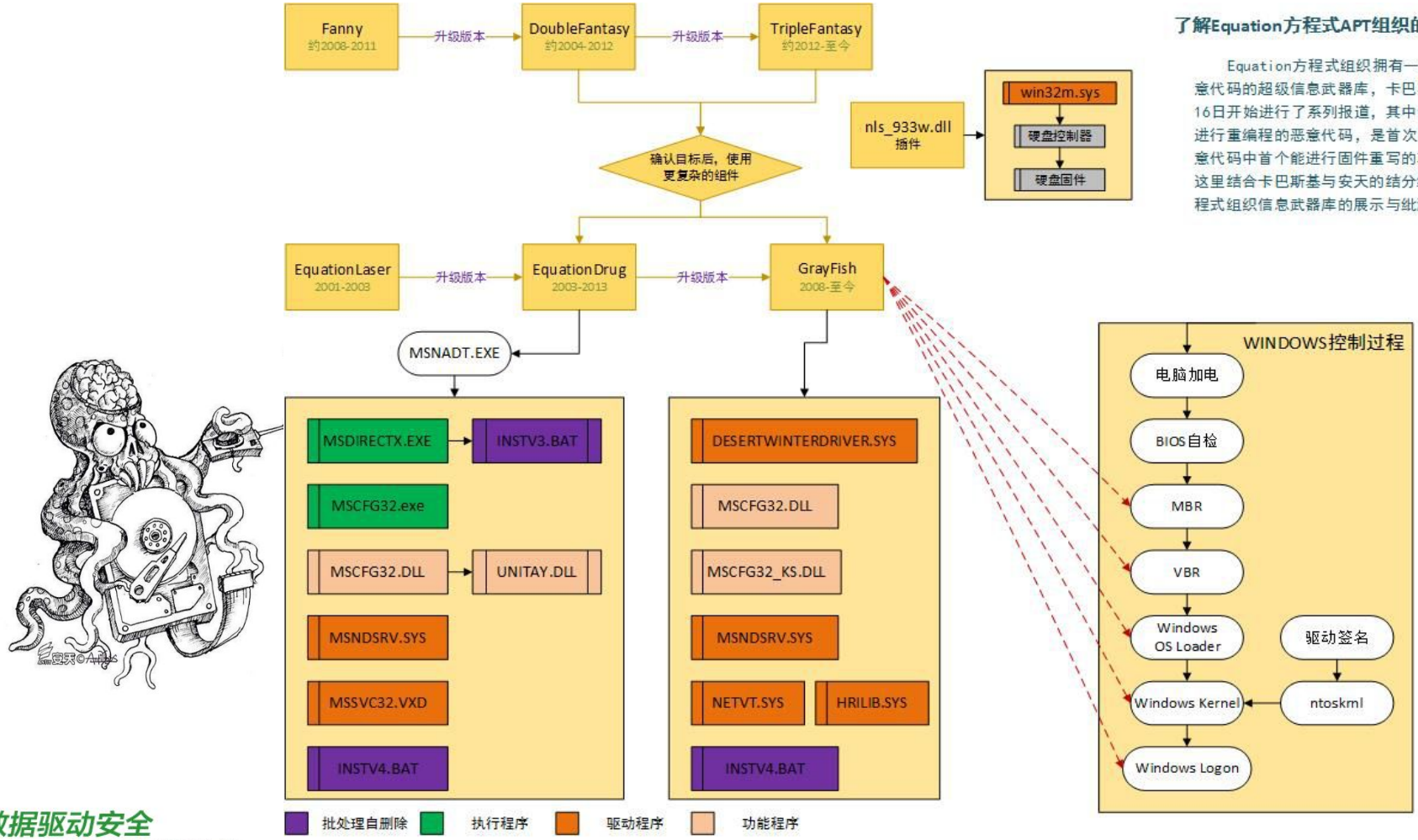
我们面对怎样的对手

组件名称	说明	时间
EquationLaser	Equation组织早期使用的植入程序，大约在2001至2004年间被使用。兼容Windows 95/98系统。	2001-2003
Fanny	创建于2008年的利用USB设备进行传播的蠕虫，可攻击物理隔离网络并回传收集到的信息。Fanny被用于收集位于中东和亚洲的目标的信息。一些受害主机似乎已被升级到DoubleFantasy，然后又升级为EQUATIONDRUG。Fanny利用了两个后来被应用到Stuxnet中的0day漏洞。	2008-2011
EquationDrug	该组织使用的一个非常复杂的攻击组件，用于支持能够被攻击者动态上传和卸载的模块插件系统。怀疑是EquationLaser的升级版。	2003-2013
DoubleFantasy	一个验证式的木马，旨在确定目标为预期目标。如果目标被确认，那么已植入恶意代码会升级到一个更为复杂的平台，如EQUATIONDRUG或GRAYFISH。	2004-2012
TripleFantasy	全功能的后门程序，有时用于配合GRAYFISH使用。看起来像是DOUBLEFANTASY的升级版，可能是更新的验证式插件。	2012-至今
GrayFish	Equation组织中最复杂的攻击组件，完全驻留在注册表中，依靠bootkit在操作系统启动时执行。	2008-至今
nls_933w.dll	修改硬盘固件的超级插件	2010-至今



商业军火带来的问题

我们面对怎样的对手

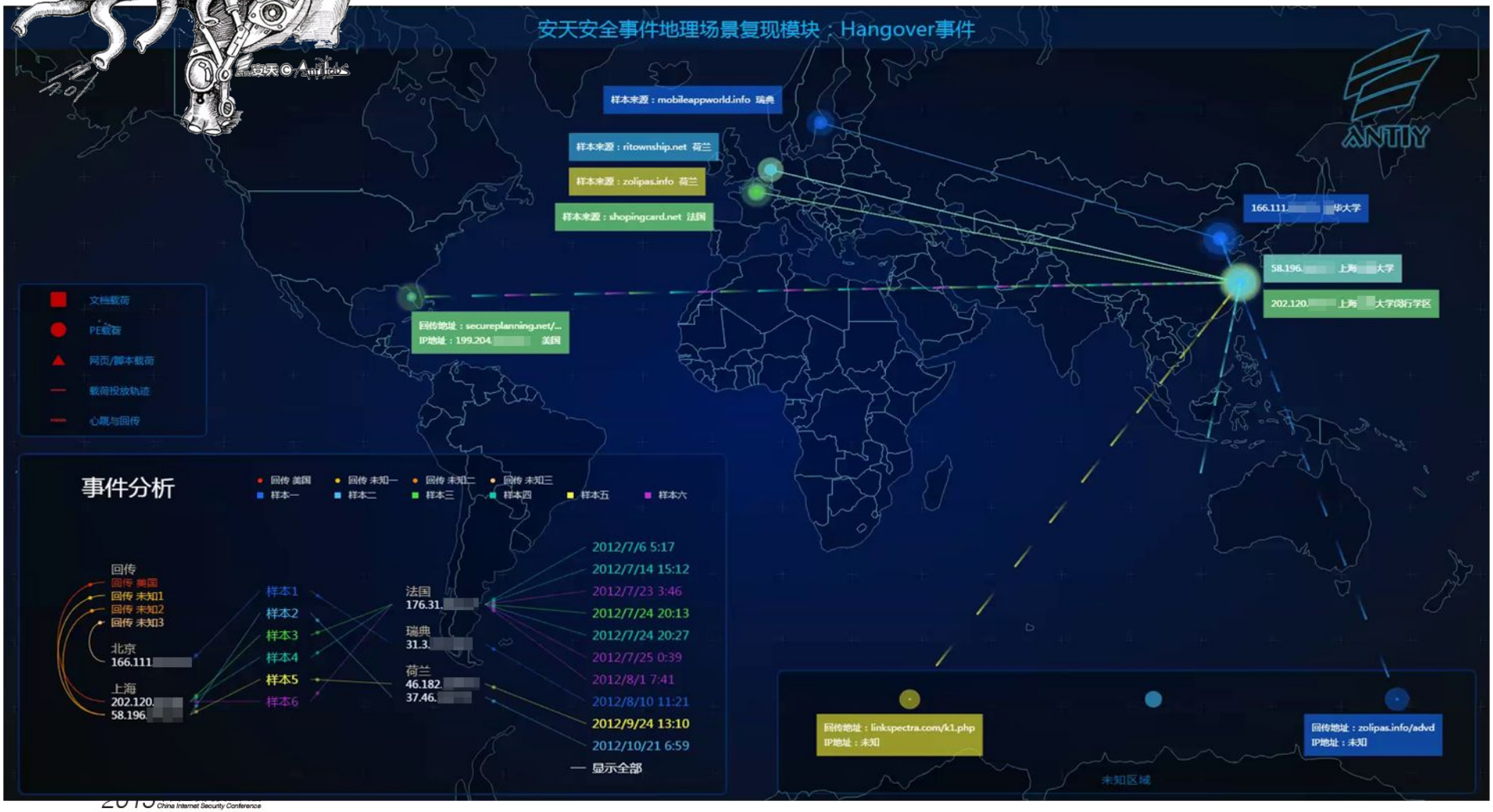


了解Equation方程式APT组织的信息武器库

Equation方程式组织拥有一套用于植入恶意代码的超级信息武器库，卡巴斯基在在2月16日开始进行了系列报道，其中针对硬盘固件进行重编程的恶意代码，是首次出现，也是恶意代码中首个能进行固件重写的功能被发现。这里结合卡巴斯基与安天的结分结果，进行方程式组织信息武器库的展示与纰漏。

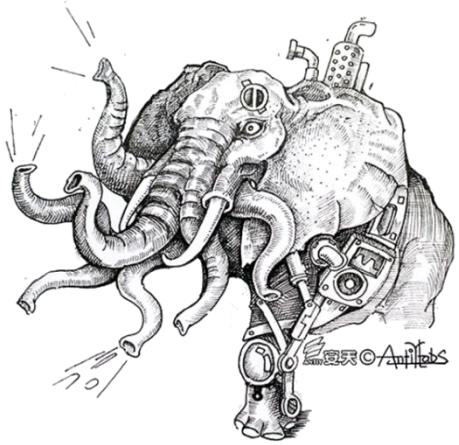
商业军火带来的问题

不同水平的攻击者



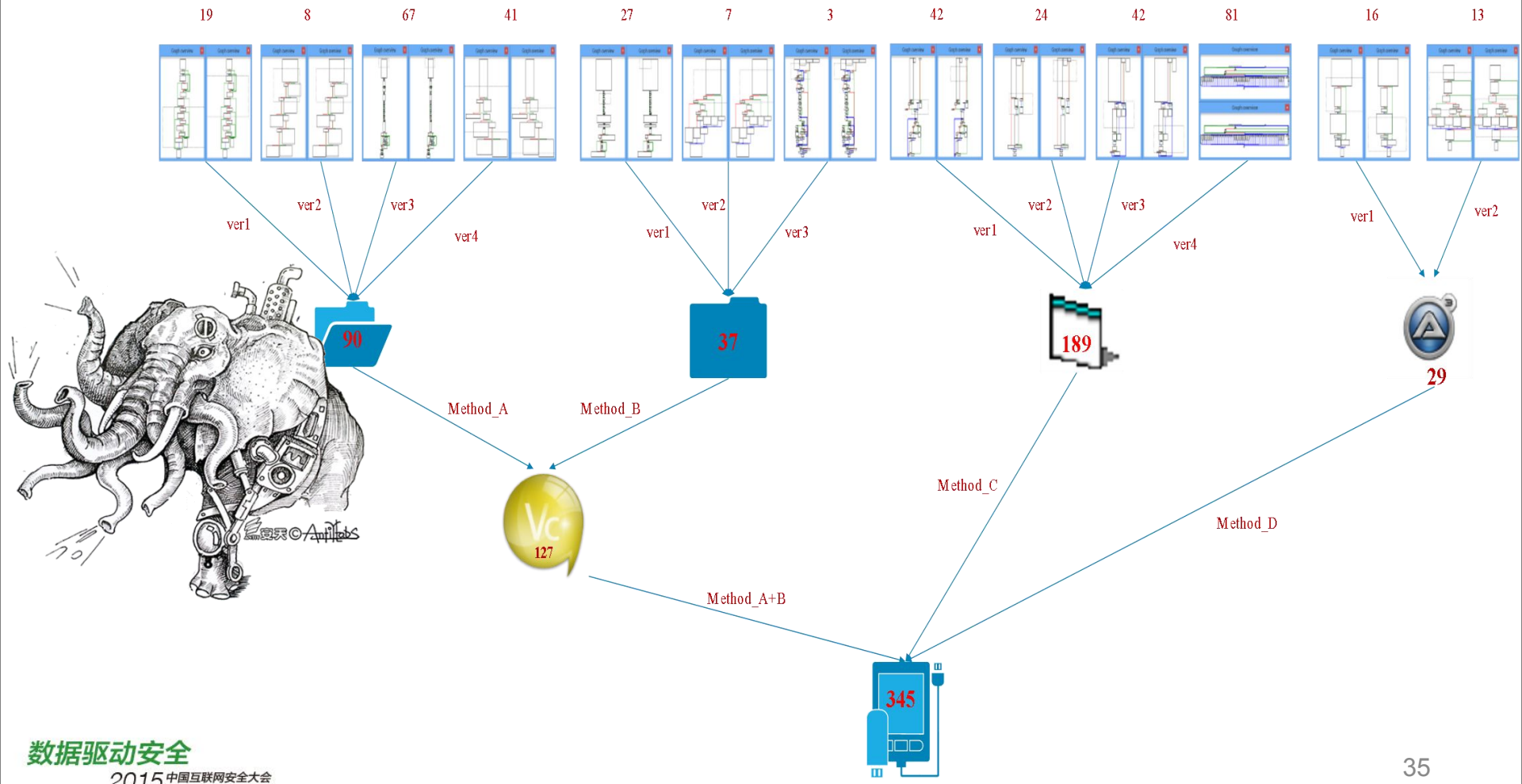
商业军火带来的问题

不同水平的攻击者



商业军火带来的问题

不同水平的攻击者



商业军火带来的问题

商业化攻击平台造成的影响

可以采取的应对策略

企业面临的窘境

共性：

- 预算有限，威胁无穷
- 多处受敌，被动防御
- 安全业务，互为制约

区别：

- 只能忍受，无力反抗

可以采取的应对策略

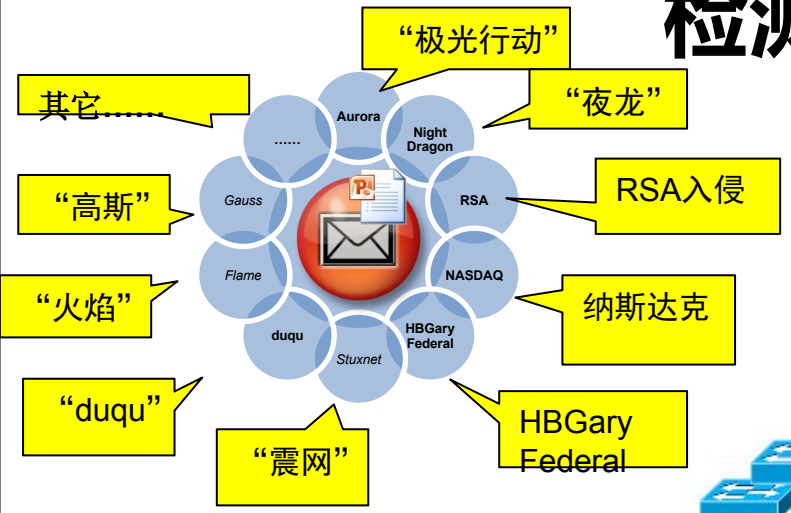
纵深防御

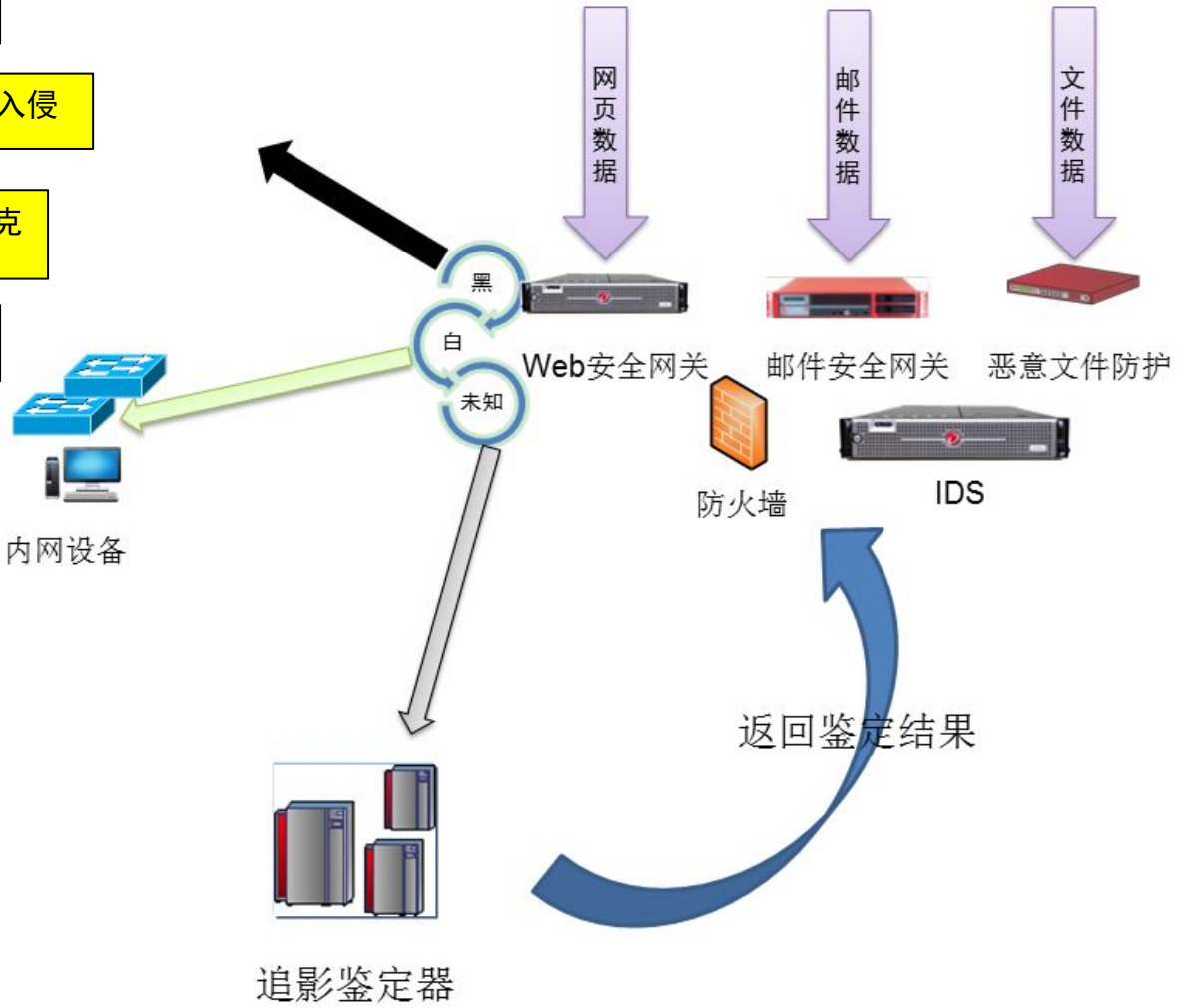
核心思路：

- 层层设防，消耗敌人
- 有效响应，不断完善

可以采取的应对策略

检测攻击源头





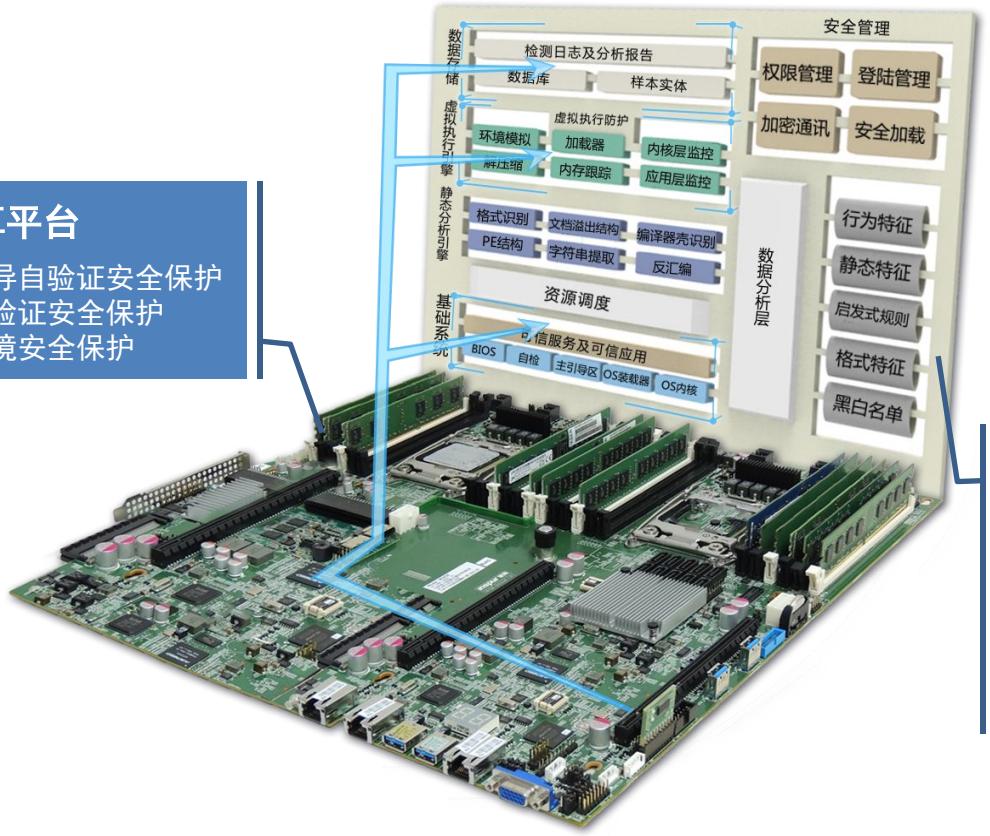
- 检测文档格式漏洞攻击
- 深度分析PE样本行为
- 有效发现0DAY
- 预警未知恶意代码
- 本地化海量规则
- 动态沙箱检测

可以采取的应对策略

安天在可信计算方面的探索

浪潮可信计算平台

- ✓ 系统启动引导自验证安全保护
- ✓ 数据存储自验证安全保护
- ✓ 虚拟系统环境安全保护



安天追影威胁分析系统（可信载体版）

- ➢ 格式文档攻击检测、PE样本深度行为分析，有效发现0DAY，预警未知恶意代码。
- ➢ 本地化海量规则和动态沙箱检测，不依赖云端能力，构建专属分析环境。
- ➢ 标准联动接口，改善安全网关、企业级安全防护产品的检测能力纵深。

inspur 浪潮

ANTIY 安天

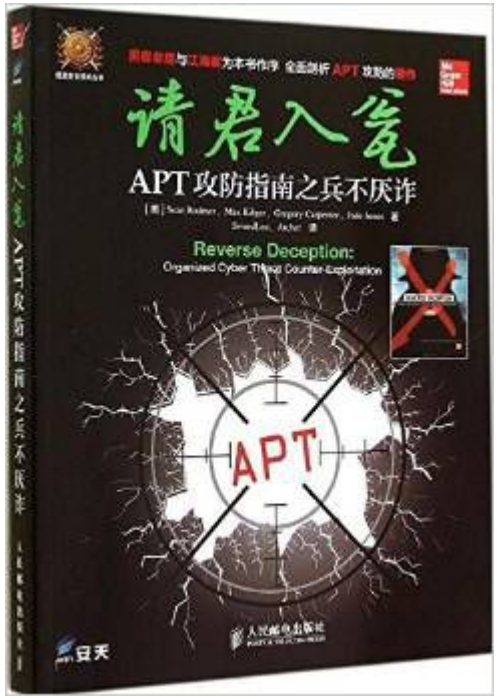
可以采取的应对策略

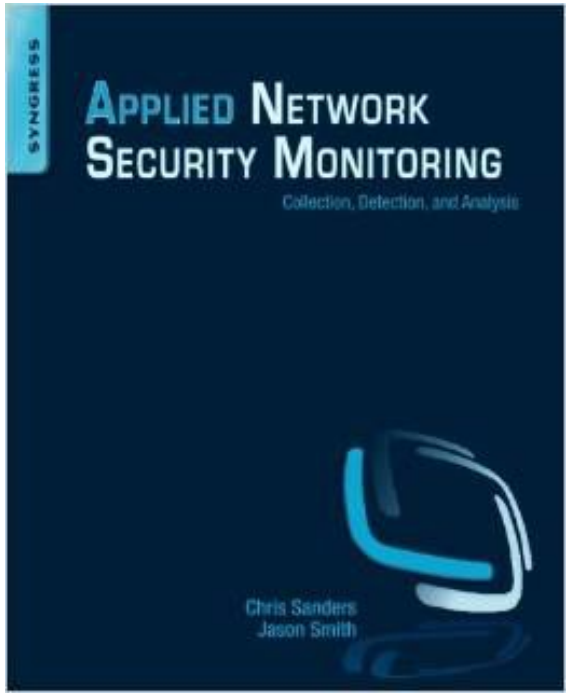
主场优势

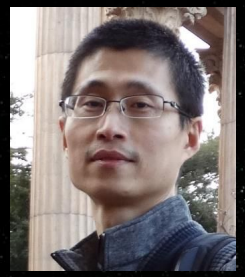
- 部署蜜罐，及时预警
- 真假难辩，迷惑对手
- 设置陷阱，追踪溯源

可以采取的应对策略

参考书目







weibo.com/libaisong75

libaisong@antiy.cn

FREEBUF

谢谢！