大型互联网企业的入侵检测

工程化下的攻防对抗

赵弼政

美团基础安全负责人

入侵案例

2010.6 **震网病毒**，伊朗核武器化进程被延缓数年

2015.3 **希拉里邮件门**，干扰总统选举结果

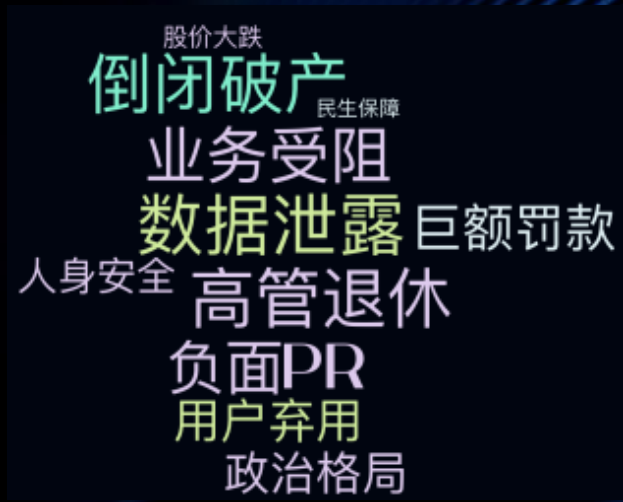
2015.7 **HackingTeam**，400G数据,7 个0day，邮件、代码、武器库泄露

2015.12 **乌克兰电网**被黑客控制关闭，2019年**委内瑞拉大停电事件**

2016.5 **孟加拉银行**指控黑客尝试转账10亿美元，成功窃取8100w美元

2016.12 **Yahoo! 被黑**，30亿账号数据，3.5亿美元

2017.5 **Equifax** 1.3亿用户数据，CEO/CIO/CSO退休，股价下跌17%



入侵的定义与特征

未经授权，强行闯入，视为入侵

闯入的对象承载企业的资产，即可能造成灾难性的后果。



ATT&CK 整理的攻击手法大盘

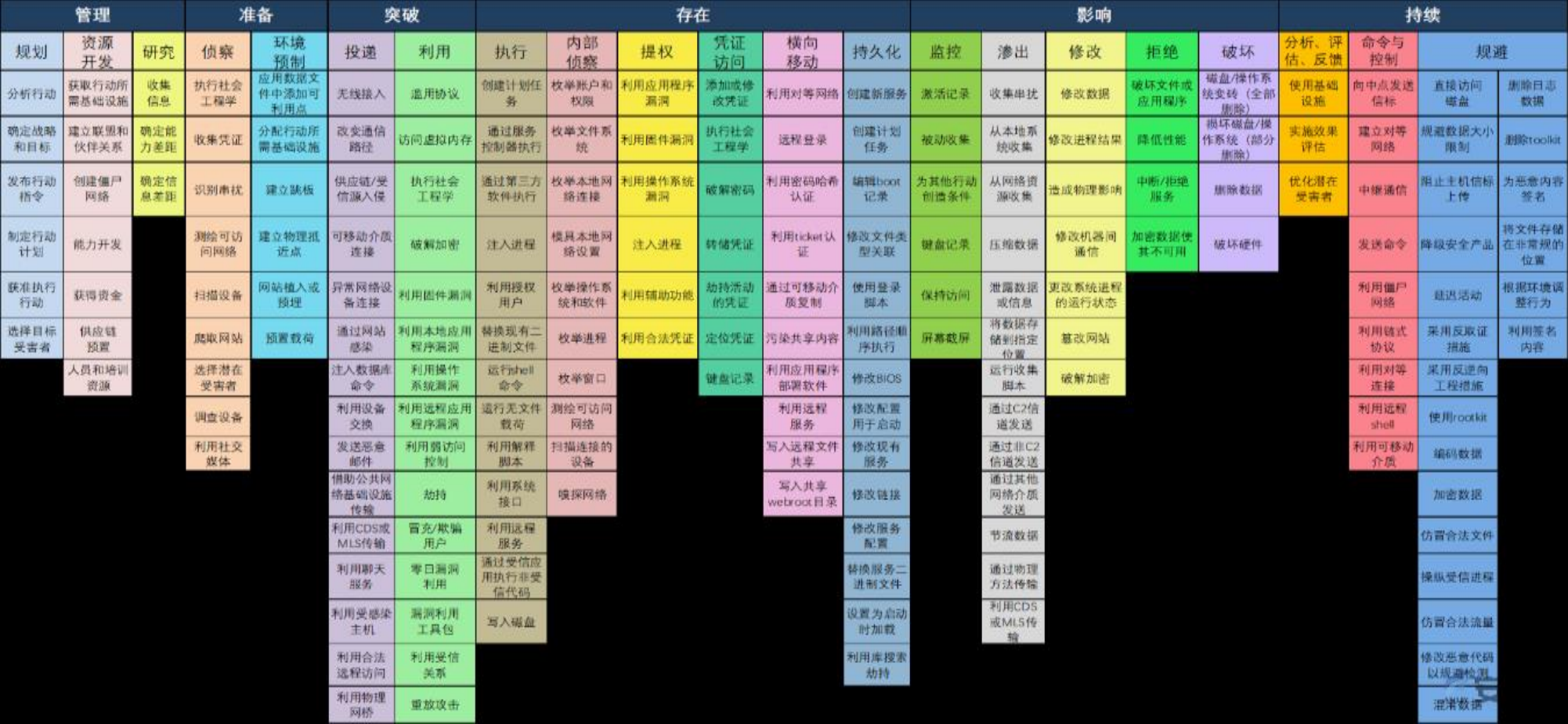
Enterprise Matrix

The full ATT&CK Matrix™ below includes techniques spanning Windows, Mac, and Linux platforms and can be used to navigate through the knowledge base.

Last Modified: 2019-04-25 20:53:07.719000

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data Staged	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Information Repositories	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Network Shared	Data Obfuscation	Exfiltration Over Other Network	Firmware Corruption

NSA/CSS技术网空威胁框架


管理
规划
资源开发
研究
分析行动
获取行动所需基础设施
收集信息
确定战略和目标
建立联盟和伙伴关系
确定能力差距
发布行动指令
创建僵尸网络
确定信息差距
制定行动计划
能力开发
获准执行行动
获得资金
选择目标受害者
供应链预置
人员和培训资源
准备
侦察
环境预制
执行社会工程学
应用数据文件中添加可利用点
收集凭证
分配行动所需基础设施
识别串扰
建立跳板
测绘可访问网络
建立物理抵近点
扫描设备
网站植入或预埋
爬取网站
预置载荷
选择潜在受害者
调查设备
利用社交媒体
突破
投递
利用
无线接入
滥用协议
改变通信路径
访问虚拟内存
供应链/受信源入侵
执行社会工程学
可移动介质连接
破解加密
异常网络设备连接
利用固件漏洞
通过网站感染
利用本地应用程序漏洞
注入数据库命令
利用操作系统漏洞
利用设备交换
利用远程应用程序漏洞
发送恶意邮件
利用弱访问控制
借助公共网络基础设施传输
劫持
利用CDS或MLS传输
冒充/欺骗用户
利用聊天服务
零日漏洞利用
利用受感染主机
漏洞利用工具包
利用合法远程访问
利用受信关系
利用物理网桥
重放攻击
存在
执行
内部侦察
提权
凭证访问
横向移动
持久化
创建计划任务
枚举账户和权限
利用应用程序漏洞
添加或修改凭证
利用对等网络
创建新服务
通过服务控制器执行
枚举文件系统
利用固件漏洞
执行社会工程学
远程登录
创建计划任务
通过第三方软件执行
枚举本地网络连接
利用操作系统漏洞
破解密码
利用密码哈希认证
编辑boot记录
注入进程
模具本地网络设置
注入进程
转储凭证
利用ticket认证
修改文件类型关联
利用授权用户
枚举操作系统和软件
利用辅助功能
劫持活动的凭证
通过可移动介质复制
使用登录脚本
替换现有二进制文件
枚举进程
利用合法凭证
定位凭证
污染共享内容
利用路径顺序执行
运行shell命令
枚举窗口
键盘记录
利用应用程序部署软件
修改BIOS
运行无文件载荷
测绘可访问网络
利用远程服务
修改配置用于启动
利用解释脚本
扫描连接的设备
写入远程文件共享
修改现有服务
利用系统接口
嗅探网络
写入共享webroot目录
修改链接
利用远程服务
修改服务配置
通过受信应用执行非受信代码
替换服务二进制文件
写入磁盘
设置为启动时加载
利用库搜索劫持
影响
监控
渗出
修改
拒绝
破坏
激活记录
收集串扰
修改数据
破坏文件或应用程序
磁盘/操作系统变砖（全部删除）
被动收集
从本地系统收集
修改进程结果
降低性能
损坏磁盘/操作系统（部分删除）
为其他行动创造条件
从网络资源收集
造成物理影响
中断/拒绝服务
删除数据
键盘记录
压缩数据
修改机器间通信
加密数据使其不可用
破坏硬件
保持访问
泄露数据或信息
更改系统进程的运行状态
屏幕截屏
将数据存储到指定位置
篡改网站
运行收集脚本
破解加密
通过C2信道发送
通过非C2信道发送
通过其他网络介质发送
节流数据
通过物理方法传输
利用CDS或MLS传输
持续
分析、评估、反馈
命令与控制
规避
使用基础设施
向中点发送信标
直接访问磁盘
删除日志数据
实施效果评估
建立对等网络
规避数据大小限制
删除toolkit
优化潜在受害者
中继通信
阻止主机信标上传
为恶意内容签名
发送命令
降级安全产品
将文件存储在非常规的位置
利用僵尸网络
延迟活动
根据环境调整行为
利用链式协议
采用反取证措施
利用对等连接
采用反逆向工程措施
利用远程shell
使用rootkit
利用可移动介质
编码数据
加密数据
仿冒合法文件
操纵受信进程
仿冒合法流量
修改恶意代码以规避检测
混淆数据

入侵检测方法论的演进


1980
1986
1987
1990
1991
1998
2015
NSA提出
用户访问日志
文件访问日志
系统事件日志
首个IDS模型
规则
异常检测
神经网络
不可能检测到所有入侵
资源所需量会大量增加
用户行为顺序的异常检测
NIDS原型诞生
Snort诞生
IoT的关注
机器学习的引入

入侵检测的本质：采集数据标记异常

数据结构化

- 主机（HIDS\EDR\DLP\AV）
- 网络（NIDS\TIP）
- 数据库（DBAudit）
- 应用日志（AD\Exchange）
- 安全产品（FW\WAF）
- 运行时环境(RASP)
- 沙箱
- 威胁情报

模型

- 签名/模式匹配
- 异常
- 行为链（关联）
- ATT&CK matrix

响应

- 准备
- 识别
- 抑制
- 根除
- 恢复
- 复盘

CMDB/ITSM、大数据平台（分析引擎）、覆盖率、数据完整度、联动/行为分析

入侵检测的代价很昂贵

大型互联网企业信息资产庞大
数十万/百万计的OS、Docker实例
数以万计的雇员、办公终端
数以亿计的代码
数以千计的项目数
数以百次的日迭代
涵盖几乎所有主流技术栈中间件
日志量级在数百T/日
告警数量数以万计

中小企业
没有/个位数的安全专家
无力承担安全产品的成本
生存优先，安全靠后

残酷的真相：无论大中小企业，安全投入的资源远远不足以应付高级入侵

工程能力决定入侵发现效果

数据完整度
- HIDS/EDR/DLP/AV覆盖率
- 系统调用/运行时环境
- NIDS数据完整度
- 日志完整性
- 重点业务日志 …

场景覆盖度
- 历史案例TTPs覆盖
- ATT&CK 关键路径覆盖
- 收敛攻击面加固运营

闭环率
- 极低的误报容忍
- 可解释/可行动
- 追溯/应急平台化

应对之道

ATT&CK的1个techniques
面向公众的服务包罗万象
试图全覆盖会筋疲力尽。

对外：高危端口 + Web攻防
对内：失陷假设 + 横向移动
全网蜜罐(HIDS、EDR)
重点系统纵深防御
AD、邮件、知识库
运维平台、Agent平台
攻击尝试
. . .

Exploit Public-Facing Application

The use of software, data, or commands to take advantage of a weakness in an Internet-facing computer system or program in order to cause unintended or unanticipated behavior. The weakness in the system can be a bug, a glitch, or a design vulnerability. These applications are often websites, but can include databases (like SQL) [1], standard services (like SMB [2] or SSH), and any other applications with Internet accessible open sockets, such as web servers and related services. [3] Depending on the flaw being exploited this may include Exploitation for Defense Evasion.

For websites and databases, the OWASP top 10 and CWE top 25 highlight the most common web-based vulnerabilities. [4] [5]

最低成本防御/检测

管理			准备		交互		存在						影响					持续		
规划	资源开发	研究	侦察	环境预置	投放	利用	安装、执行	内部侦察	提权	凭证访问	横向移动	持久化	监控	渗出	修改	拒绝	破坏	分析、评估、反馈	命令与控制	规避
N/A			高危端口管理		WAF 命令 RASP		Webshell\扫描\蜜罐 提权\异常登录\C2 EDR\系统调用分析						N/A					C2		

效果展示：大事件里的小失误

震网病毒：自动感染内网其它机器符合扫描特征
Equifax： Struts S02-045，Java启动异常子进程
HackingTeam：nmap慢速扫描、pwdump/mimikatz、AD非预期登录、AD管理员登录员工机器

【NIDS 端口扫描告警】
2019-05-10 10:35:45从OA网发起的流量监测到北京-xx办公网172.x.x.x(zhangsan/张三) 自 2019-05-10 10:33:36起对10.x.x.x进行了PortScan,端口数量达到161个,触发规则10次,涉及敏感端口 80,1080

【HIDS发现疑似恶意进程】

2019-05-27 14:33:26 jenkins-slave-test193 〔内网服务〕触发了[Java命令执行]规则，符合[目录探测]特征。

进程用户：jenkins
PID：294373
命令：pwd
父进程：java -Dsun.jnu.encoding=UTF-8 -Dfile.encoding=UTF-8 -jar slave.jar -jnlpUrl http://
祖父进程：python local.py

从0开始建设怎么做


迭代优化
高运营标准下建模
• 日均误报在个位数
• 杜绝Key-Value，鼓励自然语言
• 工单化、移动化、平台化
采集数据
• agent研发（HIDS\EDR）
• NIDS研发（suricata）
• WAF日志采集（进出数据）
• DNS数据采集（NIDS解析、日志服务器）
• 应用日志采集（AD、Exchange）
• 内部服务日志采集（SSO、知识管理平台、运维/代码仓库日志）
• 基础设施数据推进

总结

1. 入侵很可怕，危害很大
2. 入侵检测的代价很高，大型企业有资源，但依然不够，应主动追求ROI
3. 入侵检测的方法论其实已成熟多年，之后演进的方向集中在数据丰富多样化、攻击场景体系化、响应过程标准化和平台化
4. 工程能力决定入侵发现效果
5. 检测思路要扬长避短
6. 维持一贯的高标准要求，很多APT也可能大意被捕获

提醒：维护公司对安全产品的信任，宁可少/漏数据，
也不要造成业务事故


THANKS
TENCENT SECURITY CONFERENCE 2019