

工程化下的攻防对抗

TENCENT SECURITY CONFERENCE 2019 2019腾讯安全国际技术峰会



# 赵弼政

美团基础安全负责人

# 入侵案例

2010.6 展网病毒,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Oday,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 Eouifax 1.3亿用户数据, CEO/CIO/C5O退休, 股价下跌17%

倒闭破产<sub>生系版</sub> 业务受阻 数据泄露巨额罚款

### 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 20:52-07 719000

ast 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 .bashro	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	Applnit 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	Applnit 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

TENCENT SECURITY CONFERENCE 2019 2019腾讯安全国际技术峰会

管理		准备		5	医破	存在								影响		持续					
规划	资源 开发	研究	侦察	环境 預制	投递	利用	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、評 估、反馈	命令与 控制	规	避
分析行动	获取行动所 需基础设施	收集 信息	执行社会 工程学	应用数据文 件中添加可 利用点	无线接入	進用协议	创建计划任 务	枚挙跃户和 权限	利用应用程序 漏洞	添加成修 改凭证	利用对等网络	创建新服务	激活记录	收集申扰	修改數据	破坏文件或 应用程序	磁盘/操作系 绕变砖 (全部 振除)	使用基础 设施	向中点发送 信称	直接访问 概象	無除日志 数据
确定战略 和目标	建立联盟和 伙伴关系	确定能 力差距	收集凭证	分配行动所 関格個设施	改变通信 路径	访问虚拟内存	通过服务 控制器执行	枚举文件系 统	利用跟件漏洞	执行社会 工程学	远程登录	创建计划 任务	被动攻集	从本地系 统收集	修改进程结果	即低性能	提环磁盘/提 作系统(部分 無除)	实施效果 评估	建立对等 网络	規避数据大小 限制	删除toold
发布行动 哲令	创建偏尸 网络	确定信 息差距	识别非权	建立誘板	供应链/受 信源人侵	执行社会 工程学	通过第三方 软件执行	枚學本地同 絡连接	利用操作系统 謝詞	60 90 90 50	利用密码哈希 认证	编辑boot 记录	为其他行动 创造条件	从网络資 源收集	造成物理影响	中斯/拒绝 服务	無務数据	优化潜在 受害者	中銀過价	附止主机信标 上传	为恶意内容 签名
制定行助计划	能力开发		測绘可访 何网络	建立物理机 近点	可移动介质连接	被解放時	注入进程	模具本地阿 络设置	注入进程	转错光证	利用ticket以 证	修改文件类 型关联	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		发送命令	降级安全产品	将文件存储 在非常规的 位實
既准执行 行动	获得资金		扫描设备	网站植入波 预埋	异常网络设备连接	利用医件漏洞	利用授权用户	枚举操作斯 统和软件	利用辅助功能	劫持活动 的凭证	通过可移动介 原复制	使用登录 脚本	似物访问	推薦数据 或信息	更改系统进程 的运行状态				利用個尸 网络	超进活动	根据环境调 整行为
选择目标 受害者	供应链 授置		腐败网站	预置数荷	通过网站 感染	利用本地应用 程序漏洞	特换现有二 进制文件	枚举进程	利用合法凭证	定位凭证	污染共享内容	利用路径順 序执行	肝寒乾肝	将数据存 锗到指定 位置	篡改网站				利用链式 协议	采用反取证 措施	利用签名 内容
	人员和培训 資源		选择潜在 受害者		注人数据库 命令	利用操作 系统测润	运行hell命令	枚举窗口		键盘记录	利用应用程序 部署软件	传改BIOS		运行收集 胸本	破解加密				利用対等连接	采用反逆角 工程措施	
			調查设备		利用设备 交换	利用過程应用 程序漏洞	运行无文件 载荷	測绘可访问 网络			利用进程服务	條效配置 用于启动		通过C2倍 道发送					利用选程 shell	使用rootkit	
			利用社交 媒体		发送恶愈 邮件	利用弱访问 控制	利用解釋	扫描连接的 设备			写入远程文件 共享	修改现有 服务		通过非C2 倍道发送					利用可移动 介质	编码数据	
					併助公共同 格基础设施 传统	A019	利用系统接口	嗅探网络			写入共享 webrock目录	修改链接		通过其他 网络介质 发送						加密数据	
					利用CDS或 MLS传输	智克/欺骗 用户	利用近程 服务					修改服务 配置		节流数据						仿置合法文件	
					利用聊天 服务	零日期別 利用	通过受信应 用执行车受 信代码					特換服务二 进制文件		通过物理 方法传输						操纵使信进程	
					利用受感染 主机	期到利用 工具包	写入假盘					设置为启动 計加载		利用CDS 成MLS传 验						仿實合法流量	
					利用合法 选程访问	利用受信 关系						利用库搜索 劫持								修改图章代码 以现 <b>避</b> 检测	
					利用物理 网桥	重放攻击														泥湖数据	

## 入侵检测方法论的演进



## 入侵检测的本质:采集数据标记异常

#### 数据结构化

- ・主机 [HID5\EDR\DLP\AV] ・网络 [NID5\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/IT5M、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O5、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



HID5/EDR/DLP/AV覆盖率 系统调用/运行时环境 NID5数据完整度 日志完整性 重点业务日志 … 历史案例TTPs覆盖 ATT&CK 关键路径覆 盖 收敛攻击面加固运营 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[HID5、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						1/1
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
	Π/.	A		5端 管理	命	AF 令 SP	拐	ebsh 是权\ DR\.	异常	登:	录\ <i>C</i>	2			N/A				Cz	

## 效果展示:大事件里的小失误

展网病毒、自动感染内网其它机器符合扫描特征 Equifax: Struts 502-045, Java启动异常子进 是

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0A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Port5can,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



#### 运营标准下建模

- 日均误报在个位数 · 杜绝Key-Value, 鼓励自然
- 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〕
- DN5数据采集 (NID5解析、日志服务器)
- 应用日志采集 [AD、Exchange] • 内部服务日志采集 [550、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
- 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

