

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

股价大跌

倒闭破产

民生保障

业务受阻

数据泄露 巨额罚款

人身安全

高管退休

负面PR

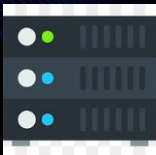
用户弃用

政治格局

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.

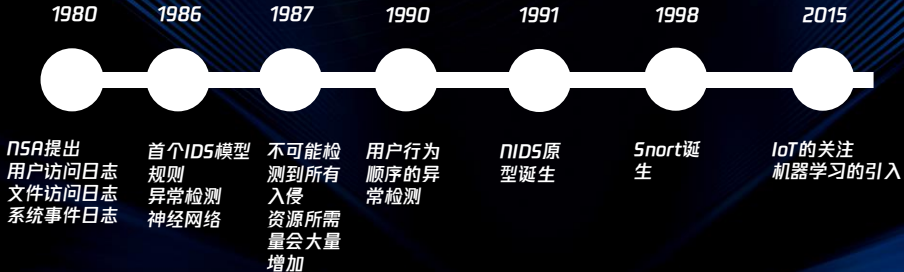
Last Modified: 2019-04-25 20:53:07.719000

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

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

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 [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



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 502-045, **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 -jnlplUrl <http://>
祖父进程: python [local.py](http://)

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

The background is a dark blue gradient with a futuristic, digital aesthetic. It features a central glowing circular interface with concentric rings and a bar chart-like pattern. Radiating lines of light extend from the center towards the corners, creating a sense of depth and motion.

THANKS

— TENCENT SECURITY CONFERENCE 2019 —