看雪

SDC·2019

2019 安全开发者峰会

Security
Development
Conference

新威胁对策：TSCM | 技术反窃密

RC²反窃密实验室
RC² TSCM LAB

Longas_杨叔

1 2019，新威胁趋势
New Trend of Threats

源码泄露 | Source Code Leaks

Real Cases

2018	Apple’s IOS source code leak
2018	Snapchat source code
2017	Drone maker DJI
2017	Microsoft Windows 10 source code leak
2013	Adobe and 30 other associated companies
2012	Symantec source code leak
2011	RSA SecureID token source code leak

商业窃密 | Theft of Trade Secrets

全美企业由于窃密导致的年度损失：

$50 billion USD

From The U.S. Chamber of Commerce
数据来自2019美国商会报告

商业窃密 | Theft of Trade Secrets

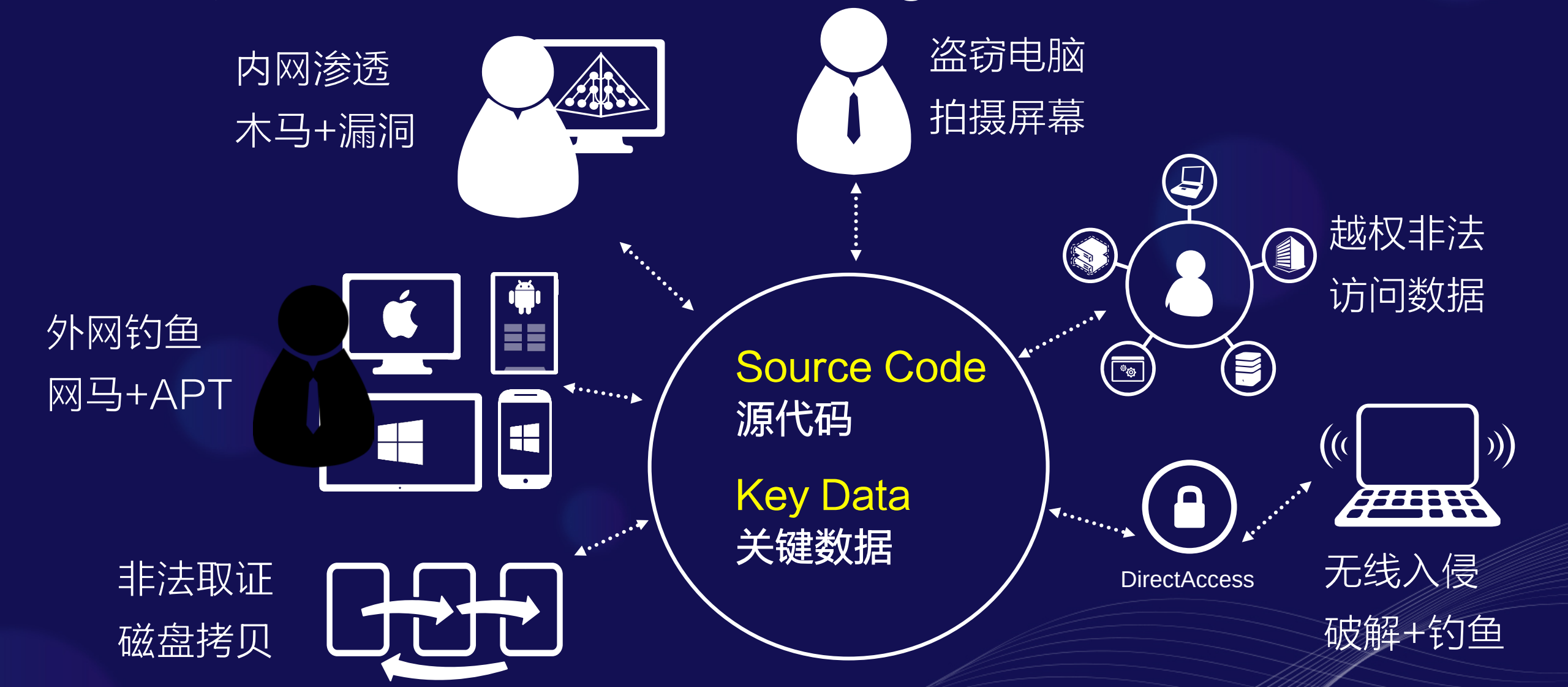
Intelligence
商业情报

Digital Core Data
企业核心数据

会议资料　销售资料　员工资料　数据库　源代码　高层资料　财务资料

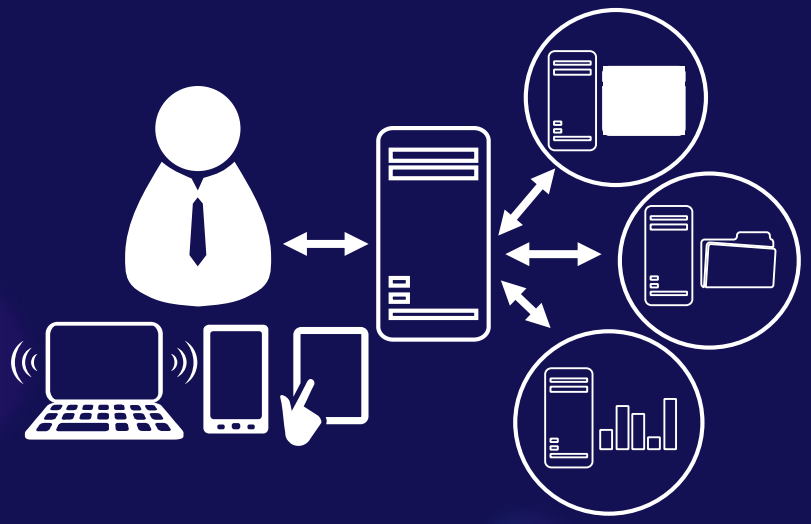
2 典型·技术窃密手段
Technical Surveillance

通用窃密手段 | General Illegal Measures



企业内控 | Enterprise Monitor Solution

法务
内审
内控
行政
安全



- DLP
- Internal Application
- Access Control
- Phone use
- Physical Tracking
- 3rd Security Platform
- Others

技术窃密 | Typical Technical Surveillance

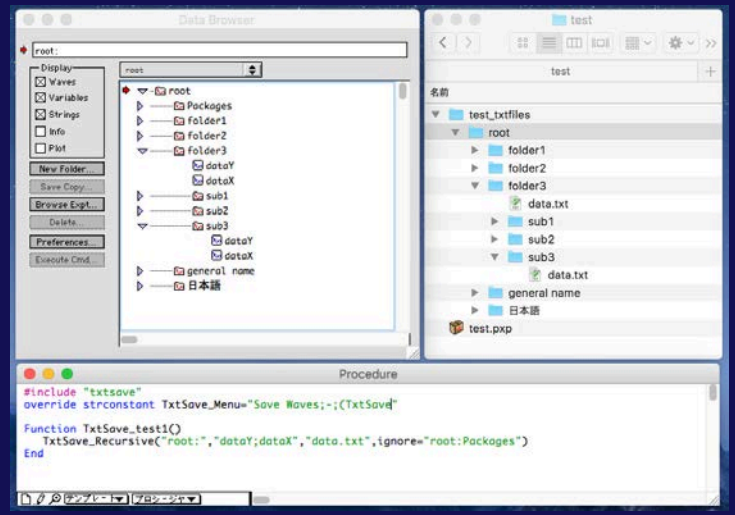
3 企业·研发环境窃密
Theft in R&D Department

本地策略规避 | Evasion Rules or Strategies

规避员工异常行为监控策略
规避电脑USB接口读写监控策略
规避外界异常声音告警策略
规避开机后自动磁盘簇检索策略
规避内部电脑截图限制策略
规避内部监控非法WiFi热点
… …

Txts to Wave

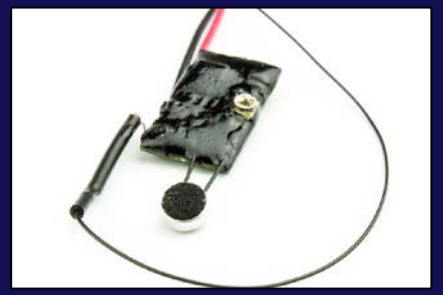
Wave to Txts



1.2GHz 无线图传

技术窃密实例 | Typical Examples

无线窃密

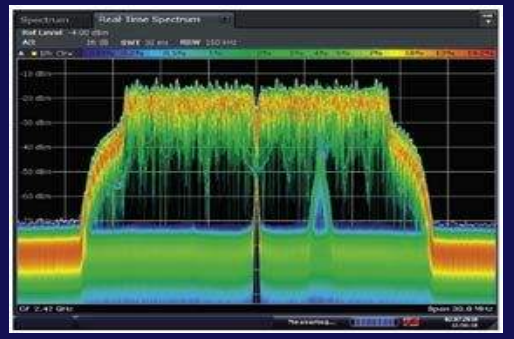


有线窃密

供应链渗透 | Penetrate the Supply Chain

窃听器材植入

信号辐射增强



电子设备改装

最终目标 Targets

高层
研发
财务
行政

供应链安全 | the Security of Supply Chain

目前中国企业

对于供应链层面窃密的防御/识别能力为：**0**

From RC² TSCM LAB
数据来自RC²反窃密实验室

4 技术反窃密
About TSCM

技术反窃密 | About TSCM

TSCM

Technical Surveillance Countermeasures

技术反窃密

指通过专业技术手段开展全方位检查，锁定并扫除一切商业级别的窃听、偷拍、偷录、跟踪定位等非法监控器材。

技术反窃密 | About TSCM

商业安全

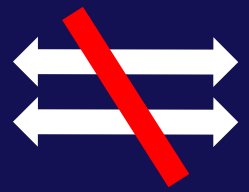
物理安全

隐私保护

跨部门

跨行业

TSCM



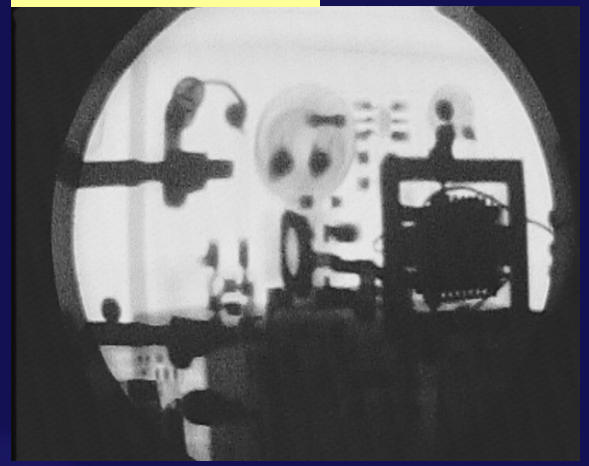
无线安全

网络安全

安保检测

技术反窃密实例 | TSCM Cases

物件透检



频谱分析

非线性检测

物理排查

WiFi识别

5 企业物理风控の要素
Physical Risk Control

企业物理风控 | Physical Risk Control

会议安防

会议前安全检测

- 确保部门内部小型项目会议安全
- 协同防守内部信息不被外泄

日常巡检

常态化安全巡检

- 确保部门主管办公室/会议室安全
- 通过日常巡检增强威慑

物理风控

物理层面风险控制

- 防物理渗透/商业刺探/访客越位
- 促进物理层面的风险隔离

隐私合规

推动隐私保护合规

- 内保体系合规性建设
- 内部商业安全及隐私保护意识的培养

TSCM威胁情报 | TSCM Threat Intelligence

技术情报

会议情报

竞争情报

政策法规

行业情报

器材情报

案例情报

装备情报

THANKS

技术公众号