



SDC · 2019

安全  
2019  
开发  
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



```
File.expand_path("../config/initializers/spec_helper.rb", __FILE__)
require "spec_helper"
require "rspec/rails"

require "capybara/rspec"
require "capybara/rails"

Capybara.javascript_driver = :webkit
Category.delete_all; Category.create
Shoulda::Matchers.configure do |config|
  config.integrate do |with|
    with.test_framework :rspec
    with.library :rails
  end
end

# Add additional requires below this line. For example, if you
# require a supporting ruby file with support for database
# connections, you can add:
# require "support/database"
#
# Requires supporting ruby files with support for database
# connections, etc. This directory should contain all the
# files that need to be loaded when running the tests.
#
# spec/support/ and its subdirectories. These files will
# be loaded by default. This directory should contain all the
# files that need to be loaded when running the tests.
#
# in _spec.rb will both be required when running the tests.
#
# run twice. It is recommended that you do not use this
# directory for anything other than the files listed above.
#
# end with _spec.rb. You can configure the require_paths
# option on the command line or in the config file.
#
# No results found for 'mongo'
#
# mongo
```

# 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

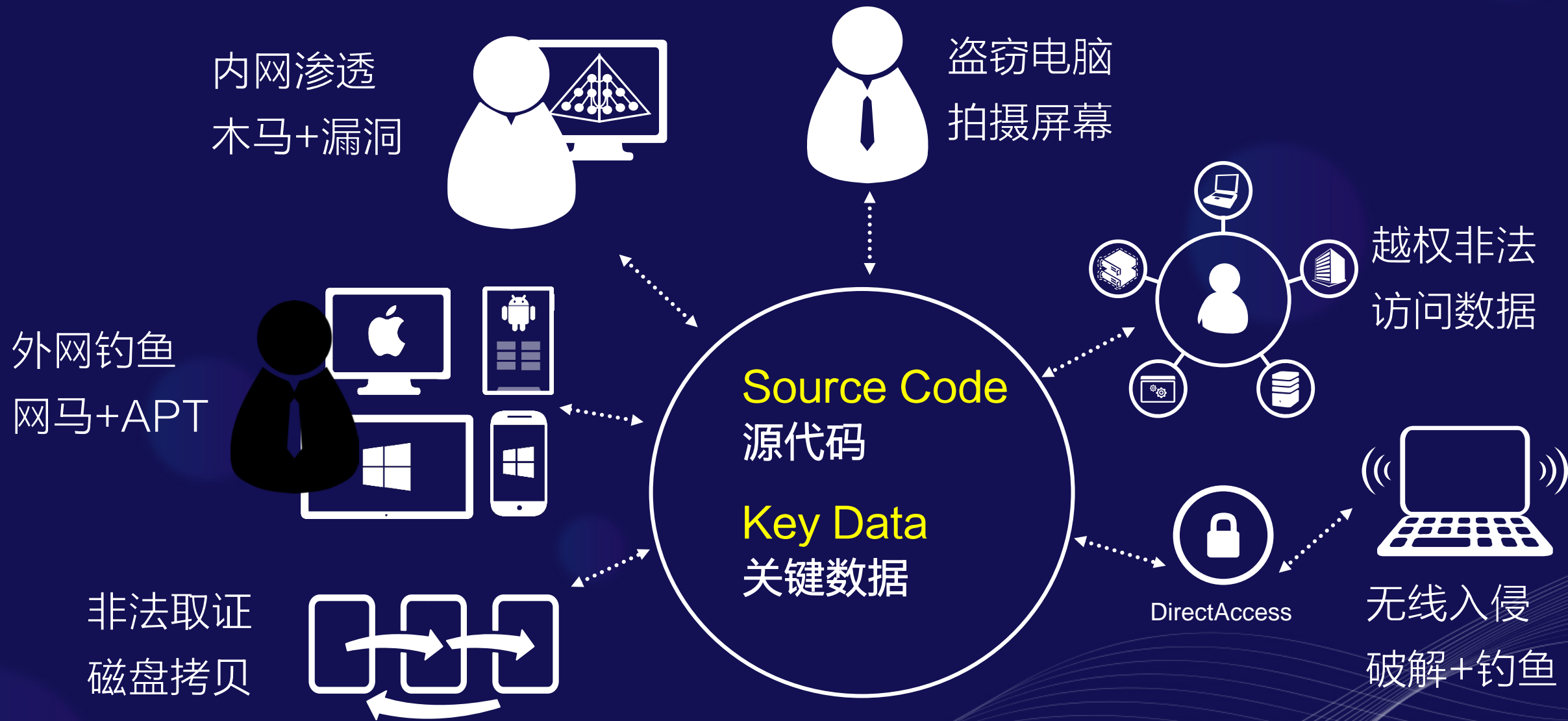




## 2

# 典型·技术窃密手段 Technical Surveillance

# 通用窃密手段 | General Illegal Measures

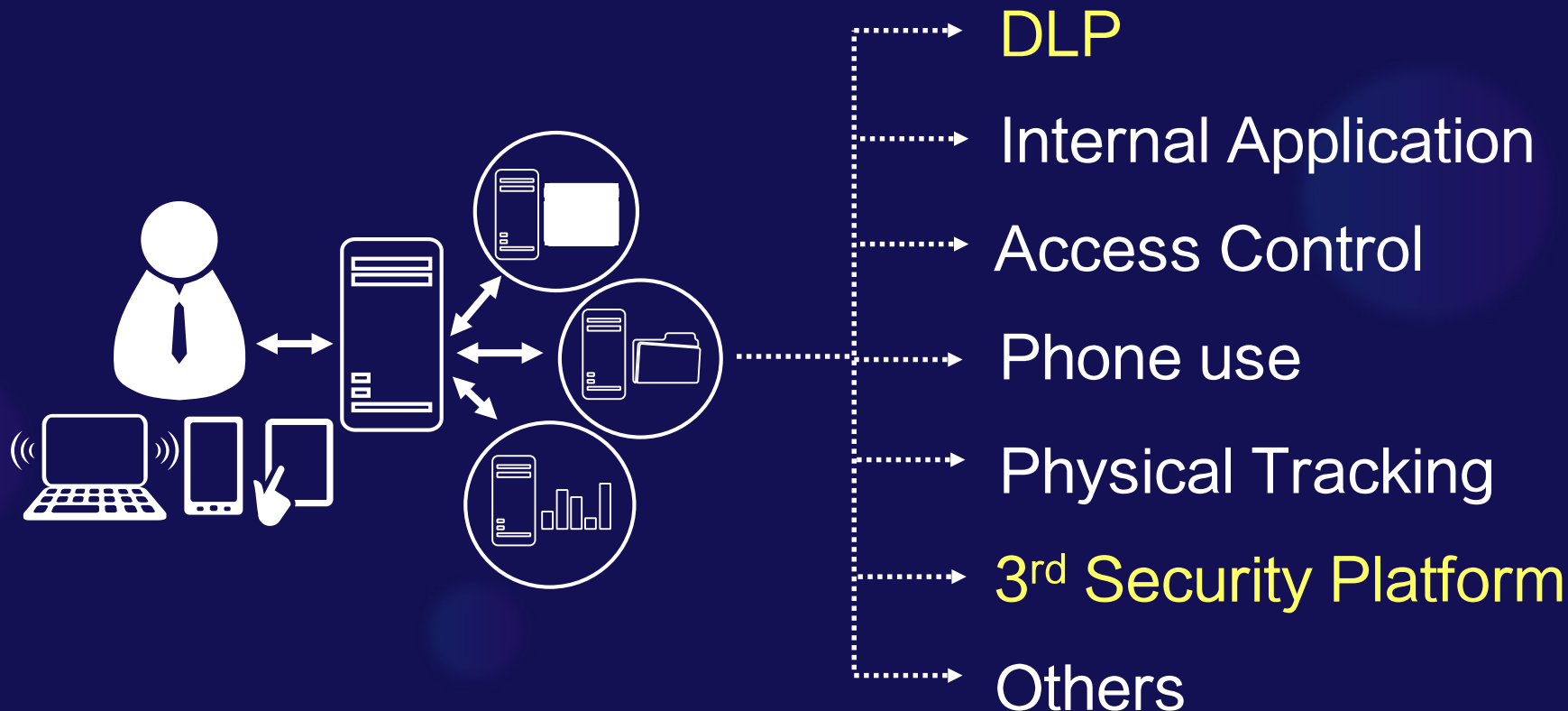






# 企业内控 | Enterprise Monitor Solution

法务  
内审  
内控  
行政  
安全



# 技术窃密 | Typical Technical Surveillance

## 无线窃密



高清无线偷拍偷录  
无线电隐秘窃听  
特殊信号频谱解析  
激光远程窃听  
...



本地策略规避  
室内线路改装  
电器摆件改装  
供应链渗透



## 有线窃密



# 3

## 企业·研发环境窃密 Theft in R&D Department

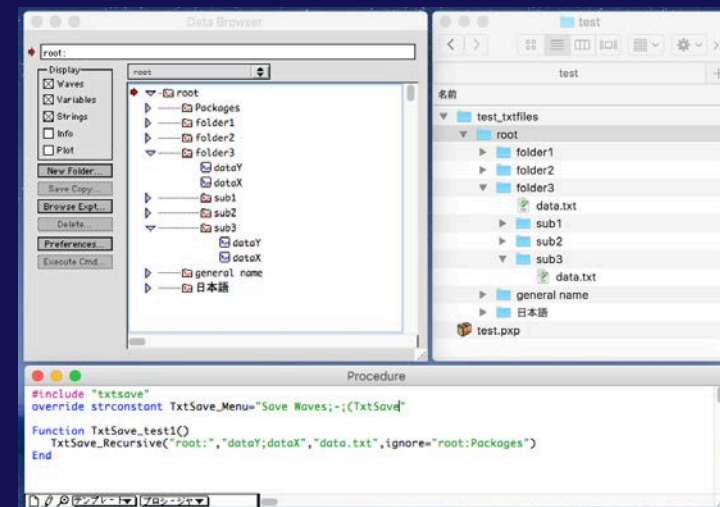


# 本地策略规避 | Evasion Rules or Strategies

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





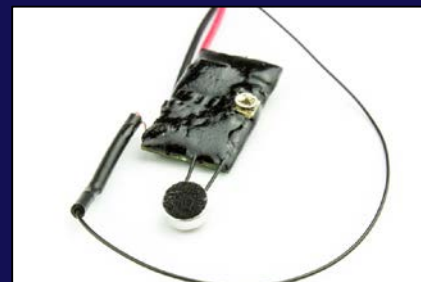


# 技术窃密实例 | Typical Examples

无线窃密



有线窃密



研 发 部

R & D DEPT.



# 供应链渗透 | Penetrate the Supply Chain



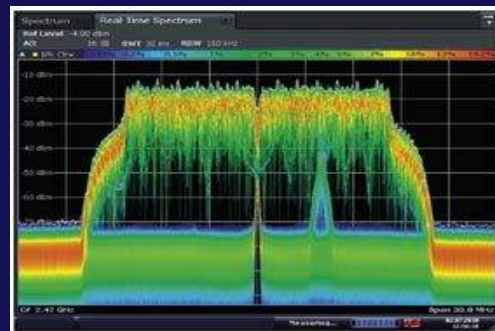
# 窃听器材植入



# 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 RC<sup>2</sup> TSCM LAB  
数据来自RC<sup>2</sup> 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

跨部门

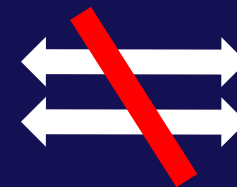
物理安全



TSCM

跨行业

隐私保护



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





2019安全开发者峰会  
2019 Security Development Conference

# TSCM威胁情报 | TSCM Threat Intelligence



技术情报

竞争情报

行业情报

案例情报

会议情报

政策法规

器材情报

装备情报





# THANKS



技术公众号