APT攻击战场升级：移动端拉响安全警报

张昊　　360烽火实验室 高级安全研究员

2018 ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018　Beijing · China
（原中国互联网安全大会）

360烽火实验室

360烽火实验室致力于Android病毒分析、移动黑产研究、移动威胁预警、Android漏洞挖掘等移动安全领域以及Android安全生态的深度研究。

实验室为360手机卫士、360手机急救箱、360手机助手等提供核心安全数据和顽固木马清除解决方案。同时也为上百家国内外厂商、应用商店等合作伙伴提供移动应用安全检测服务，全方位守护移动安全。

目录

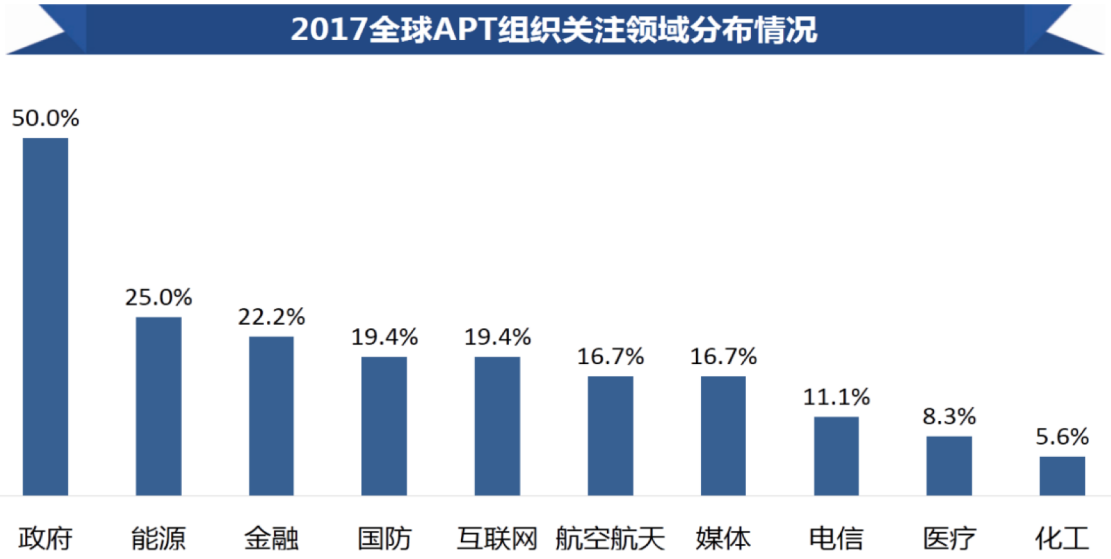
传统APT战场

传统APT战场

APT攻击（Advanced Persistent Threat，高级持续性威胁）利用先进的攻击手段对特定目标进行长期持续性网络攻击的攻击形式。

APT

被攻击目标国家	所属地区	相关报告数量	攻击组织数量
美国	北美	14	7
中国	亚洲	12	7
沙特阿拉伯	亚洲	8	4
韩国	亚洲	6	5
以色列	亚洲	5	5
土耳其	亚洲	4	2
日本	亚洲	3	3
法国	欧洲	3	2
俄罗斯	欧洲	3	2
德国	欧洲	3	3
西班牙	欧洲	2	2
巴基斯坦	亚洲	2	2
英国	欧洲	2	2



数据源：《2017中国高级持续性威胁（APT）研究报告》

传统APT战场

FANCY BEAR（奇幻熊）

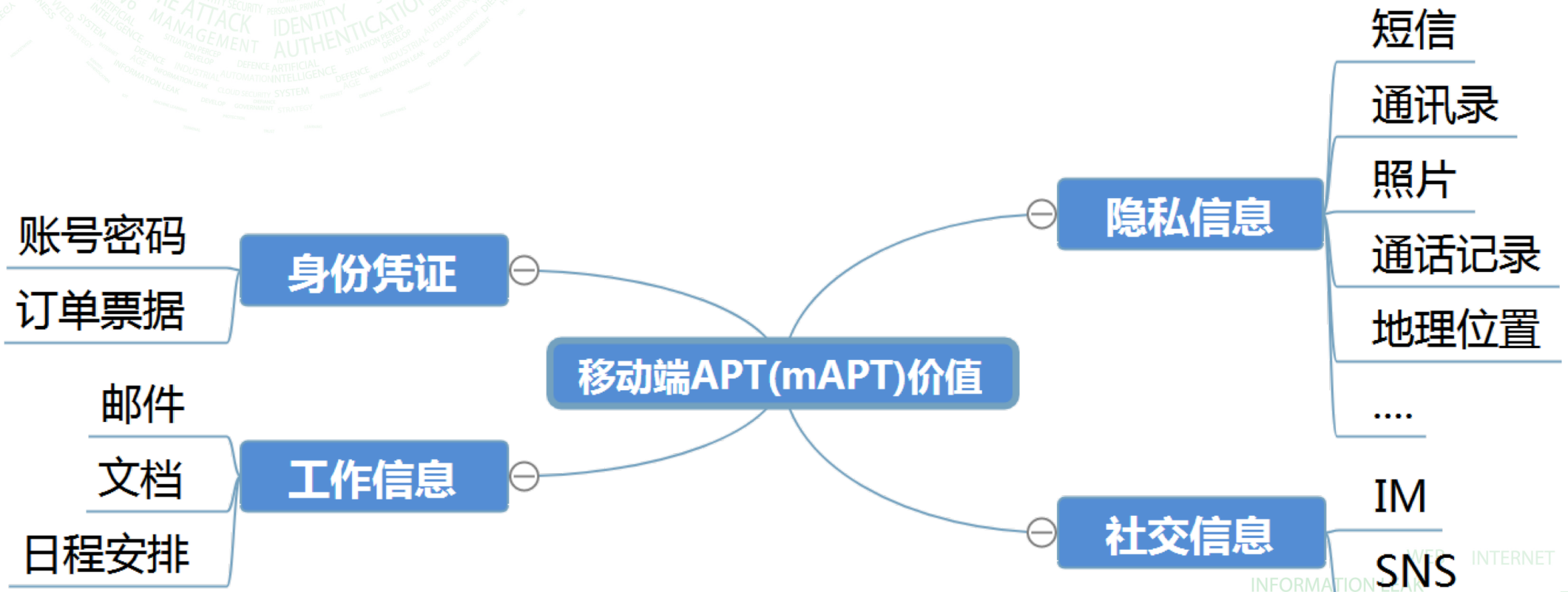
案例一： 2016年4月入侵了民主党全国委员会邮件系统，曝光了一系列丑闻，造成一直相对领先的希拉里在美国大选中失败。

案例二：伪装成合法 Android 应用程序，并秘密在乌克兰军事论坛散布。亲俄分裂分子在该恶意软件的支持下，能获得乌克兰炮兵部队的位置信息，使乌克兰炮兵部队损失一半以上的武器。

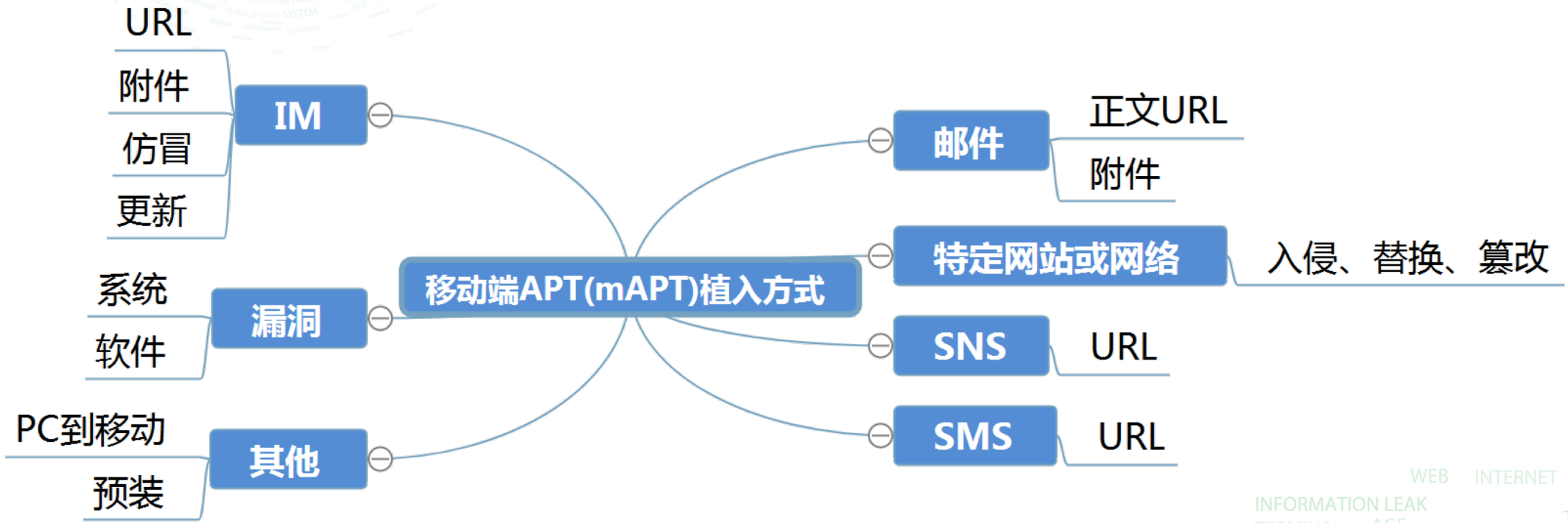
图片源： 《Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units》

新兴APT战场

移动端APT价值


移动端APT(mAPT)价值
隐私信息
短信
通讯录
照片
通话记录
地理位置
....
身份凭证
账号密码
订单票据
工作信息
邮件
文档
日程安排
社交信息
IM
SNS

植入方式


移动端APT(mAPT)植入方式
IM
URL
附件
仿冒
更新
漏洞
系统
软件
其他
PC到移动
预装
邮件
正文URL
附件
特定网站或网络
入侵、替换、篡改
SNS
URL
SMS
URL

移动端间谍类软件

	Stealing emails	Stealing surrounding voice	Stealing scheduled tasks/ calendar/ notes	Stealing social media/IM data	Backdoor behavior (e.g., remote control)	Photo/ video/ screenshot capture	Keylogging	Stealing clipboard
Pegasus	+	+	+	+	+	+	+	–
DroidJack	–	+	–	+	+	+	–	–
TiSpy	+	+	+	+	–	+	+	+
Exaspy	+	+	+	+	+	+	–	–
iKeyMonitor	+	+	–	+	–	+	+	+
Mobistealth	+	+	+	+	–	+	+	–
mSpy	+	–	+	+	+	–	+	–
iSpyoo	+	+	+	+	+	–	–	–
SpyHuman	–	+	–	+	+	+	–	–
TheftSpy	–	+	–	+	+	+	–	–
TheTruthSpy	–	+	–	+	+	–	+	–
OneSpy	+	+	–	+	–	+	–	–
Highster Mobile	+	–	–	+	–	–	–	–
Spymaster Pro	–	–	–	+	–	+	–	–
DroidWatcher	–	–	–	+	–	+	–	–

数据源：https://securelist.com/android-commercial-spyware/83098/

网络军火商

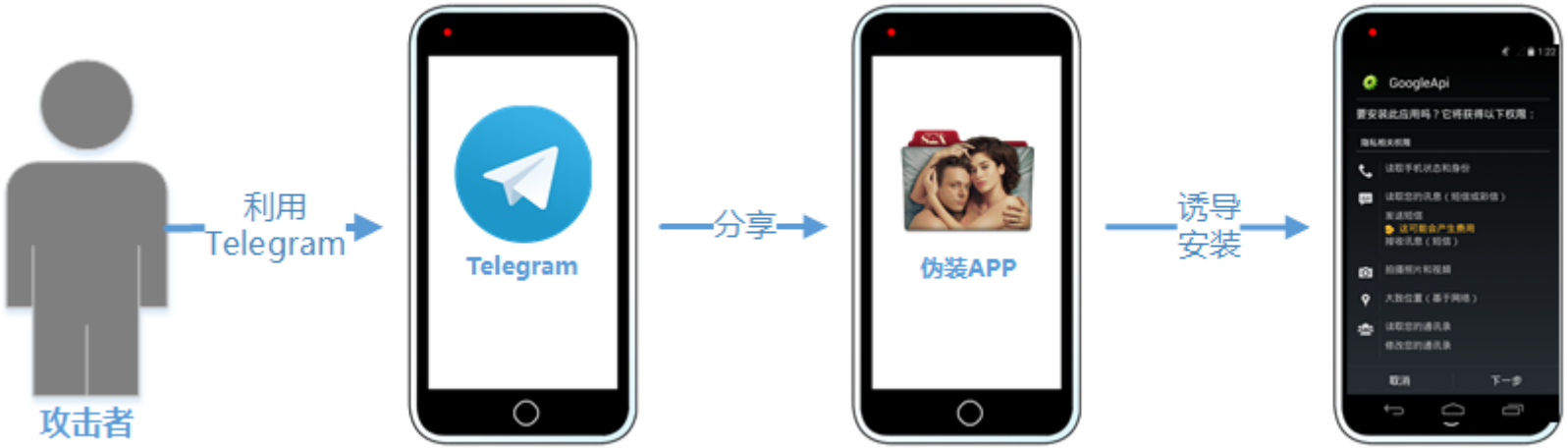
	Hacking Team	NSO Group
所在国家	意大利	以色列
服务对象	主要向政府部门及执法机构 有偿提供入侵及监视服务	主要为世界各国政府和执法机构 追踪智能手机上的任何活动
曝光事件	邮件泄露	攻击阿拉伯人权维护者
涉及平台	PC，Android，iOS， Windows Mobile，BlackBerry	Android，iOS，Blackberry
使用漏洞	TowelRoot，Framaroot	三叉戟漏洞，Framaroot
软件功能	隐私信息，社交信息 身份凭证，工作信息	隐私信息，社交信息 身份凭证，工作信息

相关案例

案例一：ARMARAT：针对伊朗用户长达两年的间谍活动

伪装对象

感染方式



案例一：ARMARAT：针对伊朗用户长达两年的间谍活动

版本变化

间谍活动使用的恶意软件分为4个版本

最早发现的版本能够伪造联系人，利用钓鱼页面，窃取Telegram账号信息，最新版本存在20多种恶意行为。

版本一

- 伪造联系人
- 窃取设备信息
- 拦截转发短信
- 静默拍照

版本二

- 隐藏图标
- 释放子包
- 窃取地理位置
- 窃取联系人
- 静默录像

版本三

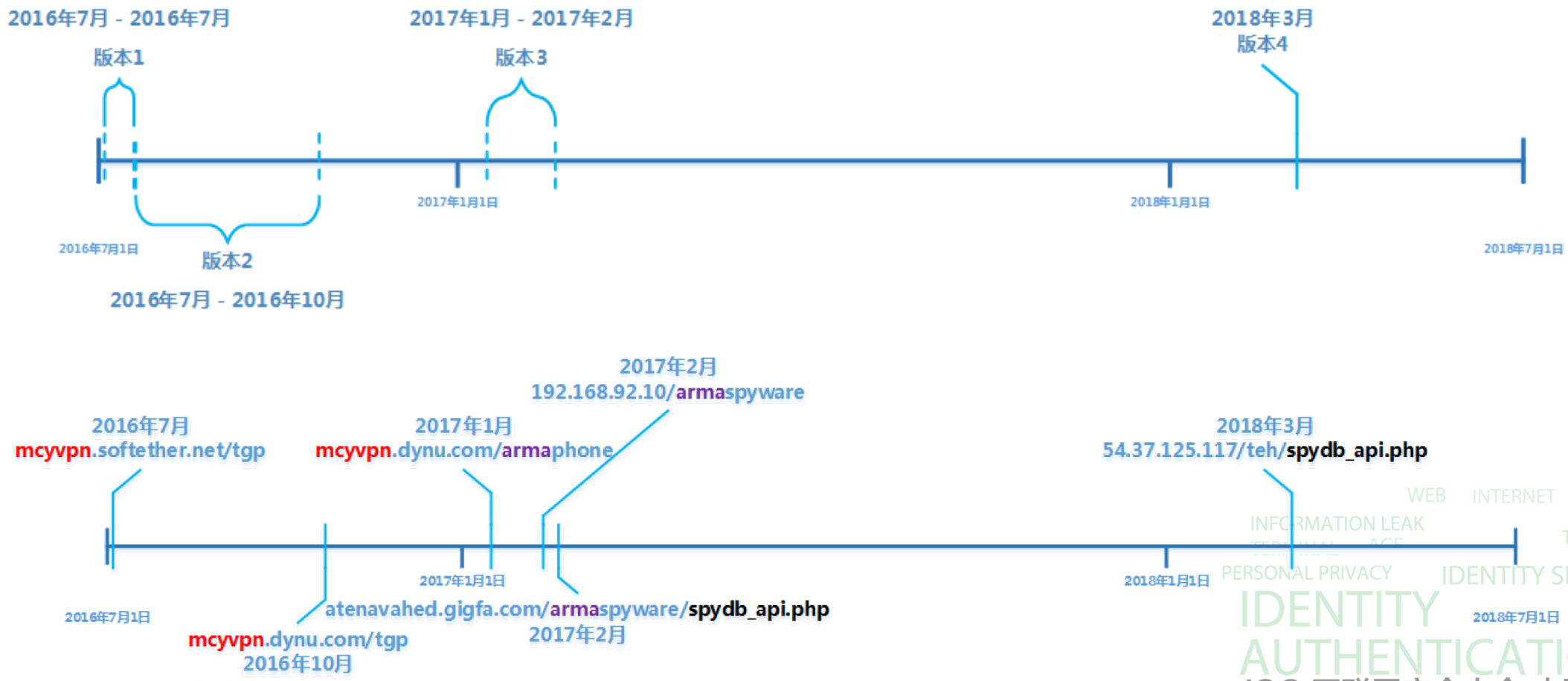
- 窃取通话记录
- 窃取短信
- 静默截屏
- 自更新
- 通话录音
- 出现关键词”armaspy”

版本四

- 窃取浏览记录
- 窃取账户信息
- 拨打电话
- 删除通话记录
- 安装列表
- 上传、下载、删除文件

案例一：ARMARAT：针对伊朗用户长达两年的间谍活动

时间维度



案例二：黄金鼠移动端跨越攻击

伪装对象

感染方式

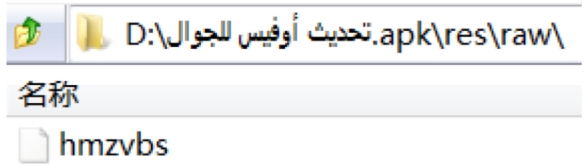
案例二：黄金鼠移动端跨越攻击

攻击步骤

步骤一：携带针对PC的PE格式RAT攻击文件

步骤二：伪装照片，图片相关目录名，扩展名为“.PIF”

步骤三：使用PC浏览手机里的照片，诱导点击触发




```
this.SpreadPIF(Environment.getExternalStorageDirectory() + "/DCIM/DCIM.PIF");
this.SpreadPIF(Environment.getExternalStorageDirectory() + "/DCIM/Camera/Camera.PIF");
this.SpreadPIF(Environment.getExternalStorageDirectory() + "/DCIM/Facebook/Facebook.PIF");
this.SpreadPIF(Environment.getExternalStorageDirectory() + "/DCIM/Screenshots/Screenshots.PIF");
this.SpreadPIF(Environment.getExternalStorageDirectory() + "/Pictures/Pictures.PIF");
this.SpreadPIF(Environment.getExternalStorageDirectory() + "/Pictures/Screenshots/Screenshots.PIF");
this.SpreadPIF(Environment.getExternalStorageDirectory() + "/Pictures/Messenger/Messenger.PIF");
```

案例小结

Fancy Bear

- 移动端和PC端独立攻击
- SNS

黄金鼠

- 移动端和PC端组合攻击
- 钓鱼页面

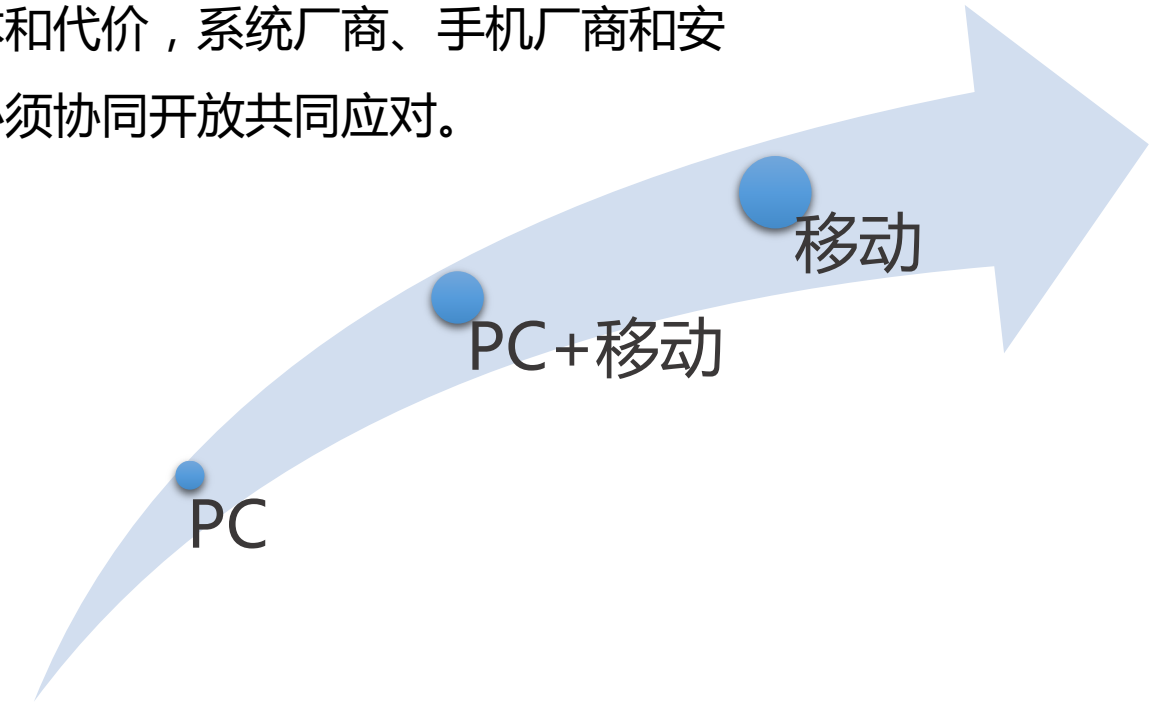
ArmaRat

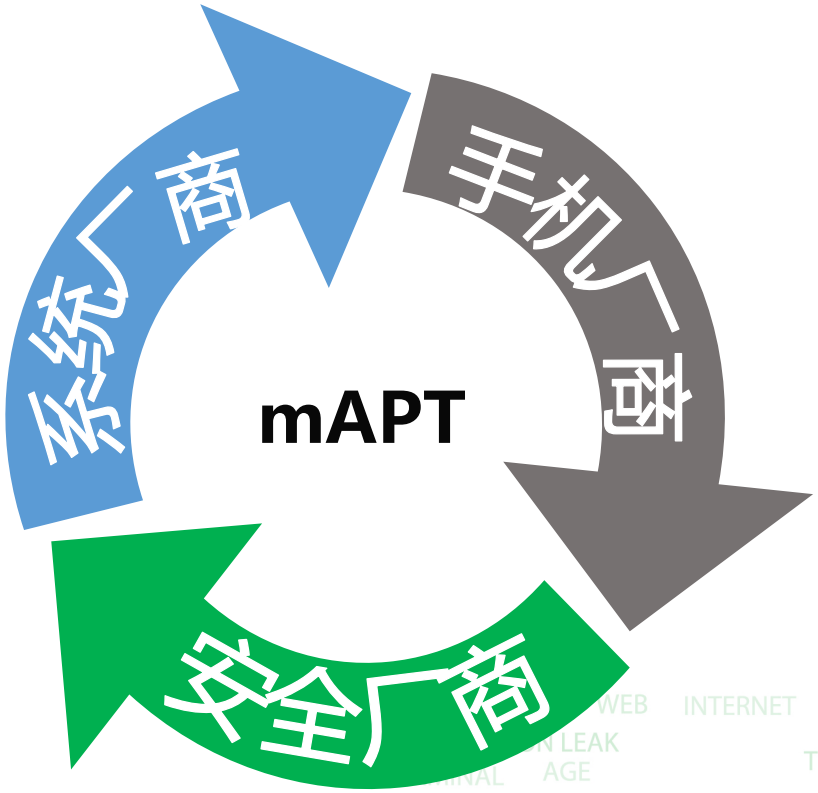
- 仅移动端
- IM

发展趋势及应对策略

黑客组织的攻击目标逐渐转向移动端，移动端或成为未来APT主要战场。

移动端的重要程度，会使得mAPT攻击不惜成本和代价，系统厂商、手机厂商和安全厂商必须协同开放共同应对。





谢 谢！

2018 ISC 互联网安全大会 中国 · 北京

Internet Security Conference 2018 Beijing · China

（原中国互联网安全大会）