Hourglass Model 2.0

Asia-based underground services abusing global 2FA

Agenda

Hourglass Model 1.0

Hourglass Model 2.0 (let's hope it is more useful)

- Generate cyber threat intelligence reports
- Actions

Case Study:

- Discovery
- Findings
- Analysis
- Conclusion: Rethink 2FA

Special Thanks

Q&A

Anna Chung

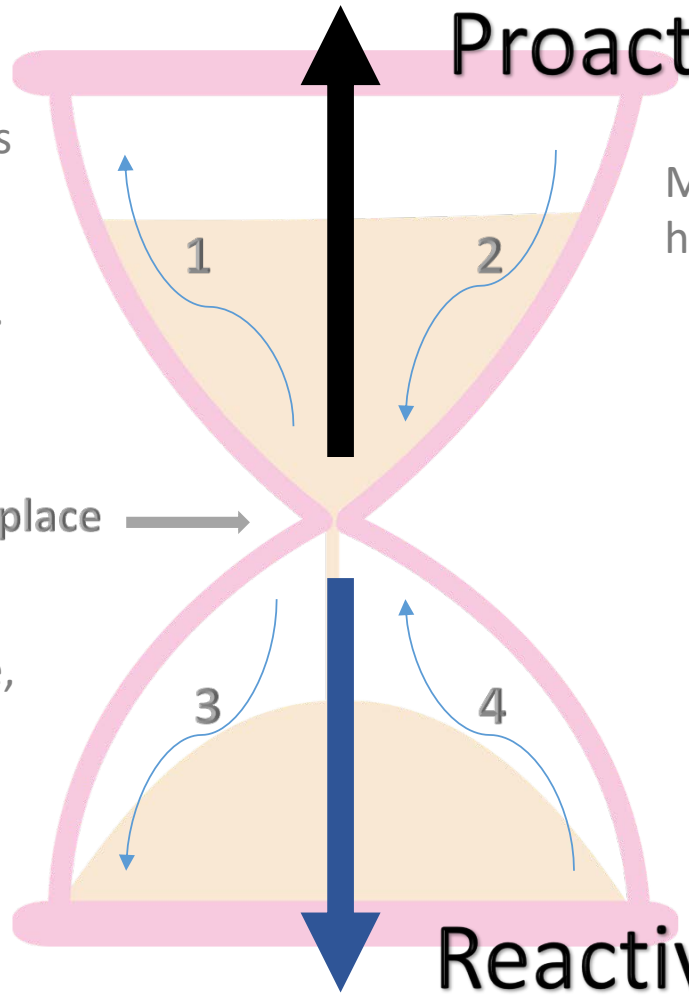
Cybercrime Researcher +7 years

International Relation background

LEGO Fan

Introduction: Hourglass Model 1.0

Cybercrime actors initiate attacks by hiring hackers, purchasing tools, exploits/malwares, and customized obfuscation services.



Malicious actors develop and provide hacking tools and services for money.

Threat actors who sell, purchase, and trade results of successful intrusion, such as login credentials, PII, shells.

Used login credentials and dataset being resell again in the underground market.

Hourglass Model 1.0: Scope

- Online activities only
- Any geolocation
- Cyber threat intelligence focus, not legal analysis
- Collection still need to abide by law and user policies!!

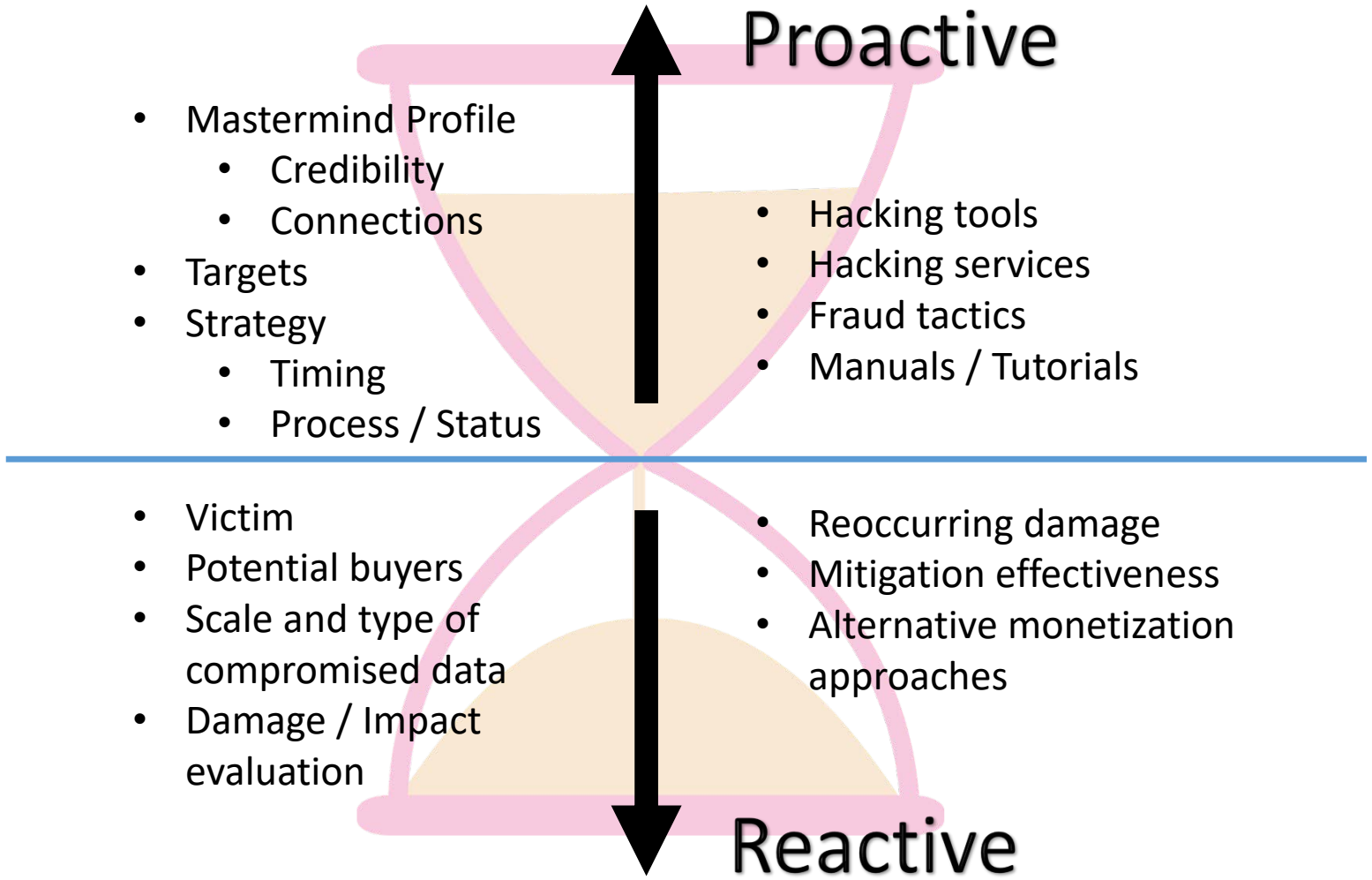
Hourglass Model 1.0: Definition of Terms

Marketplace: where communication or money flow are exchanged in the virtual world. It can be IRCs, forums, Deep and Dark Webs.

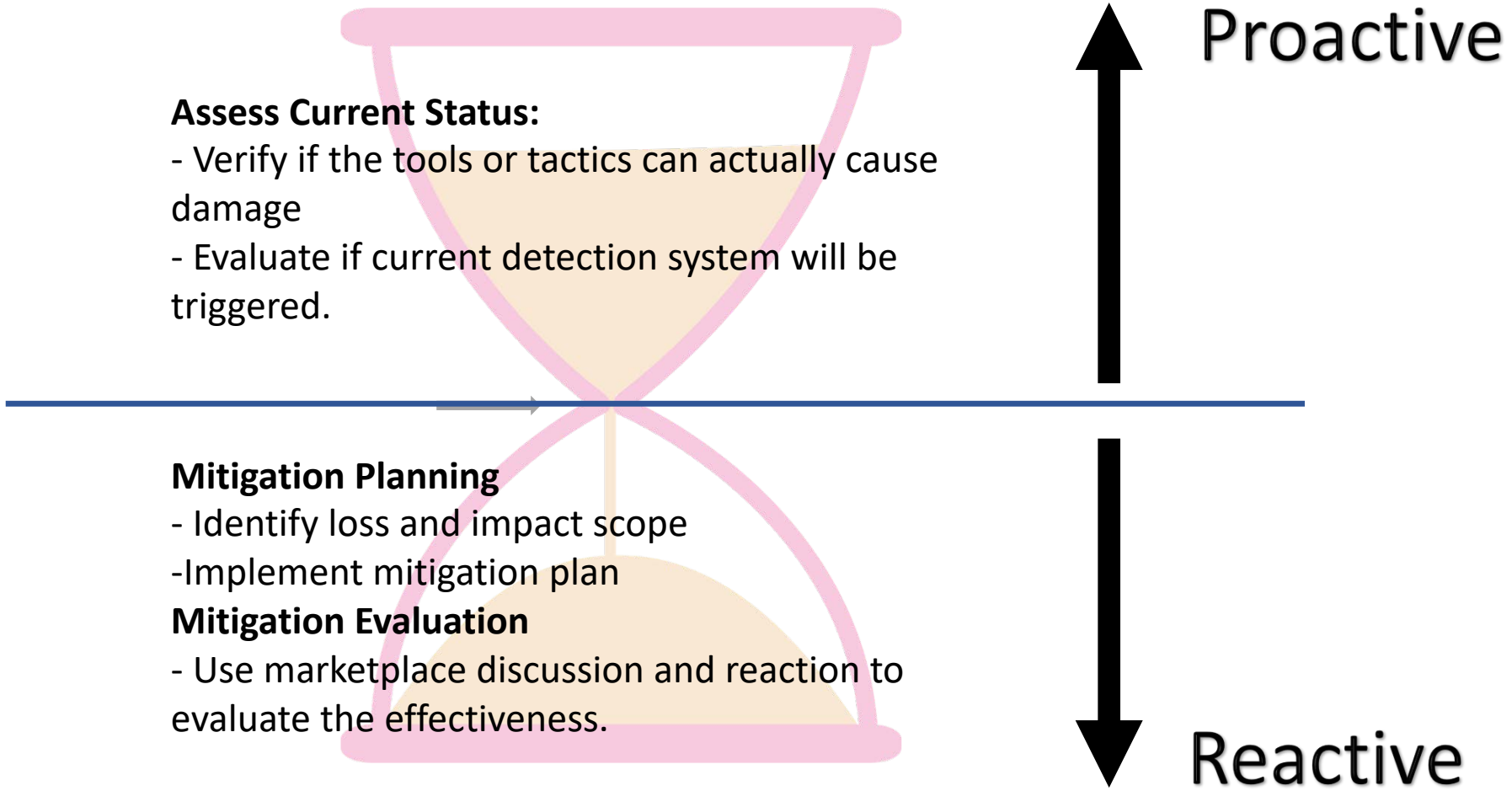
Mastermind: Threat actors with business plan and targets in mind, but still need technical assistance and others to execute the attacks.

PII: Personally identifiable information. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered PII.

Hourglass Model 2.0



Hourglass Model 2.0



Case Study

Random Discovery: Southeast Asian SIM card somehow used for abusing global eCommerce and social media

[redacted] 09:44:56

缅甸优步	1021
菲律宾优步	1029
印尼（印度尼西亚）优步	1060
俄罗斯优步	1091
柬埔寨优步	1146
菲律宾Lyft	1110
菲律宾airbnb	1052
俄罗斯airbnb	1159
柬埔寨airbnb	1170
菲律宾facebook	1077
柬埔寨facebook	1186

@全体成...

[redacted]

柬埔寨手机卡商工作室 长期稳定有卡 质量好 平台对接
可以注册 微信 淘宝 陌陌 花椒 脸书 优步 探探 映客
阿里 百度 蜜聊 line whtsapp NBN QQ 谷歌 雅虎 推特 蘑菇街等等
价格绝对优惠 另出售淘宝小号
大量柬埔寨手机卡出售 价格低到爆 有效期两个月 无限接码
有项目合作或者需要卡的也可以联系我

出售QQ提取群成员软件（可以不加群只要知道群号码就可以）QQ群发软件
大量收5S或者6苹果手机 越狱 无锁 当宝的不要！

Research Plan

- Known Information:
  - Targets/Victims
  - Underground Services

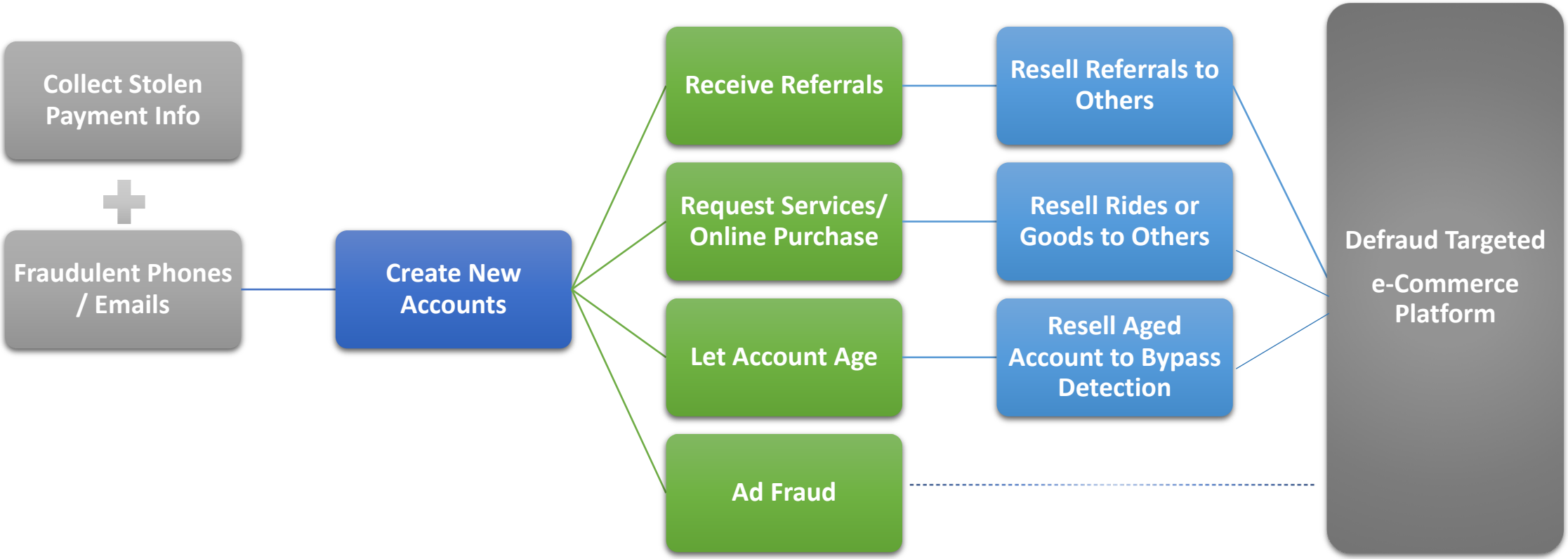
- Research Focus:
  - Identify keywords and other marketplaces to explore
  - More threat actors discuss similar topics
  - Other related underground services and goods
  - Price and availability
  - Pricing strategy
  - Tutorials
  - Potential buyers
  - Monetization workflow

Findings

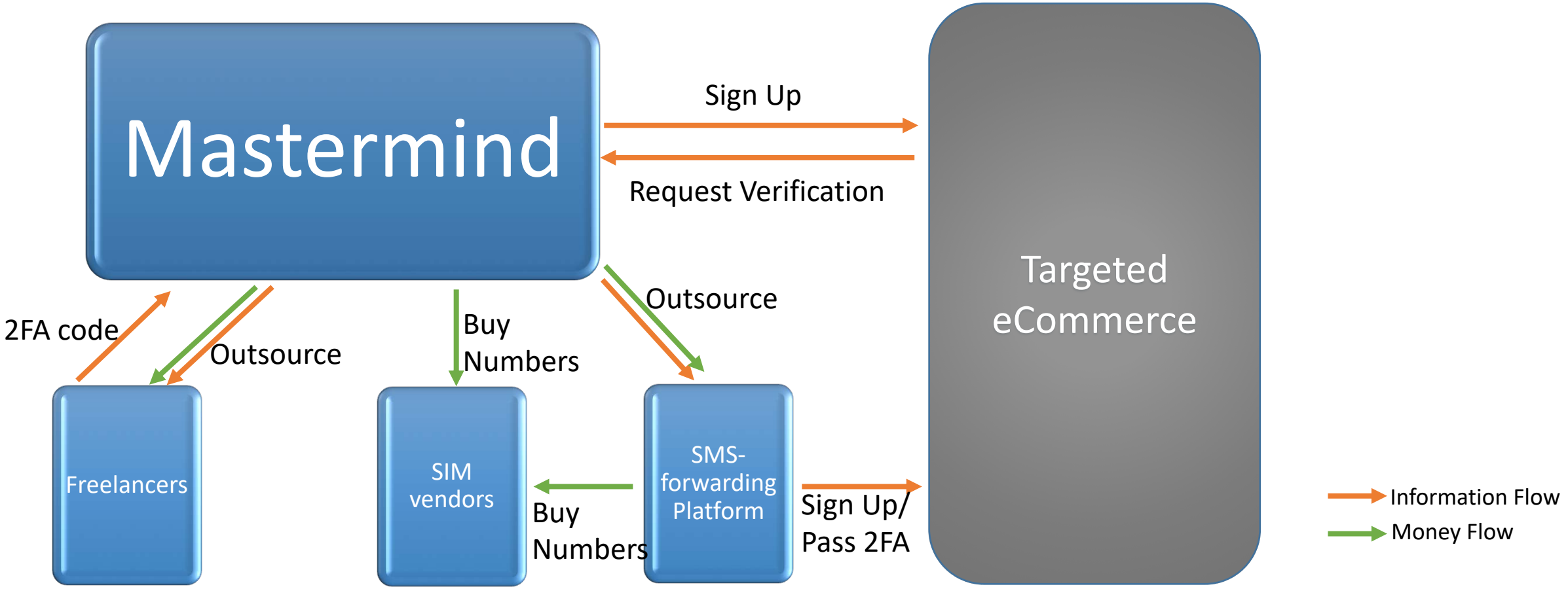

七年验证码语音验证码客户端
重新登陆
业务记录
项目信息
充 值
上线通知
公告通知
投诉建议
WEB后台
值班客服
退出软件
一号码做多项目模式
一项目多号码做模式
选择项目（可输入搜索）
语音
增加到列表
搜索
刷新数据
编号 项目名称 单价 类型
80 YY语音-比邻(禁止刷单... 0.20 多次接收
314 银联语音支付-电话支付... 0.20 多次接收
335 云微免注册语音验证码(... 1.00 语音接收
2058 TT语音帐号(禁止刷单仅... 0.20 接收
7279 阅天下语音验证码 1.00 接收
30000 陌陌语音验证码(禁止刷... 1.00 语音接收
30001 友钱语音验证码(禁止刷... 1.00 语音接收
30002 微盘宝语音验证码(禁止... 1.00 语音接收
30004 滴滴出行语音验证(禁止... 0.90 语音接收
除当前
部清除
上移
下移
（双击直接选择项目）
选择项目
关闭窗口
获取号码:
指定号码
复制
QQ发码
获取号码
切卡上线
释放号码
加黑名单
子窗口平铺
来码声音提醒
隐藏子窗口
IP
日志
09:15:02 释放号码: 15394308434 标识: 1
09:00:48 15394308434 235030--2017-12-07
09:00:11收到【知乎】创建帐号的验证码是 235030，10 分钟内有效。
09:00:13 获取号码: 15394308434
09:00:01 释放号码: 15306848619 标识: 1
08:51:08 15306848619 480467--2017-12-07
08:50:31收到【百度】欢迎注册百度帐号，您的验证码为480467，请在注册页面填写
08:50:28 获取号码: 15306848619
08:50:25 释放号码: 18157439802 标识: 1
08:50:15 获取号码: 18157439802
08:47:34 释放号码: 18380362805 标识: 1
08:47:31 获取号码: 18380362805
提示：历史日志保存在运行目录下Log.txt
清空日志框
保存调用API接口日志(API.txt)参考API开发同样功能
www.yzmpt777.com 平台相关事项可以查看这个网址
登陆帐户：247008345
帐户余额：3.15 VIP:0 折扣:无
登陆时间：2017-12-07 08:47:22
47.52.114.154


airbn优惠券
275-350
民宿优惠
请点我

Analysis I: Fraud & Monetization Flow



Analysis II: Overall Workflow

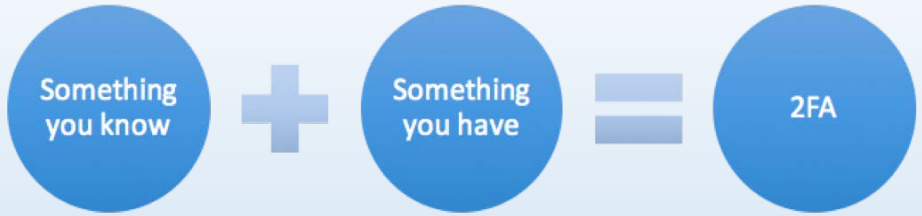


Analysis III: Other 2FA Abuse

2FA “Spamming”

- Via Email
- Via SMS

Commonly Used 2FA



Authentication via two independent components

1. **Something you know**
   a. E.g username/password combination, PIN
2. **Something you have**
   a. ***Non-online banking:*** **Mostly token-based** (device you already own, e.g cellphone)
   b. ***Online banking:*** **Mostly smartcard-based** (device which is usually provided for by bank)

Deep-dive: Cellphone-based 2FA

Exemplary authentication usage: Gmail, Instagram, iTunes purchases (optional)

- Token-based → Usually via cellphone
  a. SMS: (SMS-based authentication, e.g. TAN codes)
  b. In-App (e.g. Google Authenticator, DUO)

Risks of 2FA via SMS:

- Can be gamed by "SIM swap" (phone number redirect)
- Cell phone providers/systems can be intercepted

Re-evaluating Existing 2FA Methods

Suggested criteria for evaluating existing 2FA methods

1. **Accuracy/Security:** How accurate and secure is the 2FA system? (e.g. false/positive rates because of e.g. 2FA text message code reuse?)

1. **Online services' expertise + costs:** How technologically advanced is the deployed 2FA method and what are its costs (Cost can be a main driver to mitigate accuracy/security issues)

1. **Usability:** How easy is it for consumers to interact with the chosen 2FA method?

Deep-dive: Existing cellphone-based 2FA methods

1. **Usability**
   a. Consumer perspective: Usually 2-3 min authentication process is regarded as "acceptable" by average user.
   b. Need for balancing usability with security of chosen 2FA method

1. **Accuracy/Security**
   a. **Preferred:** In-app verification (e.g. DUO/Google Authenticator) → not affected by SIM swap attacks + increased attacker hurdle (costs for buying device + need for hacking "authentication account", e.g. Gmail for Google Authenticator)
   b. If SMS-based: No reuse of SMS 2FA codes + limited number of attempts to enter correct 2FA SMS code

2. **Online services' expertise + costs**
   a. Online services should invest in "2FA alliance models" to explore securer 2FA verification methods
   b. Methods should not bear additional costs on online services nor consumers

Hourglass 2.0 *vs* 2FA Methods

Recommendation:

Online services should adapt Hourglass 2.0 "Mastermind" knowledge transfer approach by educating their industry & consumers on 2FA authenticator apps

1. Consumers need to be educated by online services on how to use in-app 2FA

- **Video tutorial**
- **Browser notification during account setup**

2. Larger online services need to invite smaller/medium-sized online services to 2FA alliances

- **Facilitate 2FA technical knowledge transfer**
- **Shared educational resources for consumers**

TLDR – Today's Key Takeaways

- Effective cyber defense decision relies on external threat intelligence and internal data analysis.
- Hourglass model aims to help researchers maximize the information collected from marketplace information
- Use the findings to build hypothesis and evaluate existing system and policy
- Adversary will not disappear, so...use them!

Special Thanks

www.linkedin.com/in/nliguda

…to Nina Liguda - 2FA Section

Q&A