Hourglass Model 2.0

Asia-based underground services abusing global 2FA
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
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!!
**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

Proactive

- Mastermind Profile
  - Credibility
  - Connections
- Targets
- Strategy
  - Timing
  - Process / Status
- Hacking tools
- Hacking services
- Fraud tactics
- Manuals / Tutorials

Reactive

- Victim
- Potential buyers
- Scale and type of compromised data
- Damage / Impact evaluation
- Reoccurring damage
- Mitigation effectiveness
- Alternative monetization approaches

Victim
Potential buyers
Scale and type of compromised data
Damage / Impact evaluation
Reoccurring damage
Mitigation effectiveness
Alternative monetization approaches
Assess Current Status:
- Verify if the tools or tactics can actually cause damage
- Evaluate if current detection system will be triggered.

Mitigation Planning
- Identify loss and impact scope
- Implement mitigation plan

Mitigation Evaluation
- Use marketplace discussion and reaction to evaluate the effectiveness.

Hourglass Model 2.0
Case Study

Random Discovery: Southeast Asian SIM card somehow used for abusing global eCommerce and social media
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
Analysis I: Fraud & Monetization Flow

Collect Stolen Payment Info + Fraudulent Phones / Emails → Create New Accounts → Receive Referrals → Request Services/Online Purchase → Let Account Age → Ad Fraud → Resell Referrals to Others → Resell Rides or Goods to Others → Resell Aged Account to Bypass Detection → Defraud Targeted e-Commerce Platform
Analysis II: Overall Workflow

Mastermind

- Sign Up
- Request Verification
- Outsource
- Buy Numbers
- 2FA code
- Freelancers
- SIM vendors
- SMS-forwarding Platform

Targeted eCommerce

Information Flow
Money Flow

Sign Up/Pass 2FA
Buy Numbers
Outsource
Buy Numbers
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
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?)

2. **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)

3. **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
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

...to Nina Liguda - 2FA Section

www.linkedin.com/in/nliguda
Q&A