RSA Conference 2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: MBS-W03F

Upwardly Mobile: Looking at Evolving Cybercrime Tactics in Mobile Malware

John Miller

Director, ThreatScape Cyber Crime
iSIGHT Partners

#RSAC

Agenda

- Introduction
- Evolution of mobile credential theft malware
- Evolution of mobile ransomware
- Outlook and implications
- Application

Introduction | Scope

- Cyber crime: abuses of computer systems for <u>profit</u>
- Our focus: cyber criminal mobile malware

Introduction | Mobile Threat Taxonomy

GENERAL THREAT

- Call Fraud
- Phishing Email

MOBILE-TAILORED

- Phishing Sites
- Exploit Kits

MOBILE ONLY

- Malicious Apps
- SMS-Based Threats

Introduction | Mobile Malware Taxonomy

DATA THEFT	SERVICE MANIPULATION	FINANCIAL EXACTION	TRAFFIC GENERATION	ENABLING
Credential Theft	SMS & USSD Interaction	Ransomware	DDoS	Self-Spreading
SMS Interception	Click Fraud	Fake AV	TDoS	Loader
Spyware / RAT	Premium Number Fraud			Privilege Escalation
	Appstore Purchases			

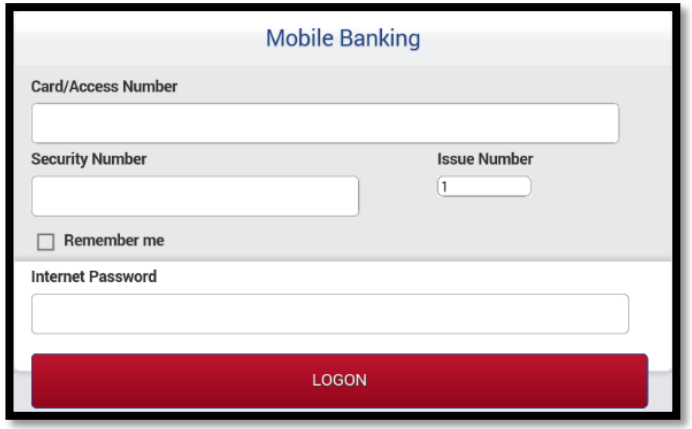
DISTRIBUTION

Illicit App Hosting	Disguised App	Malicious Update	Supply Chain

Introduction | Focus

Mobile Credential Theft Malware

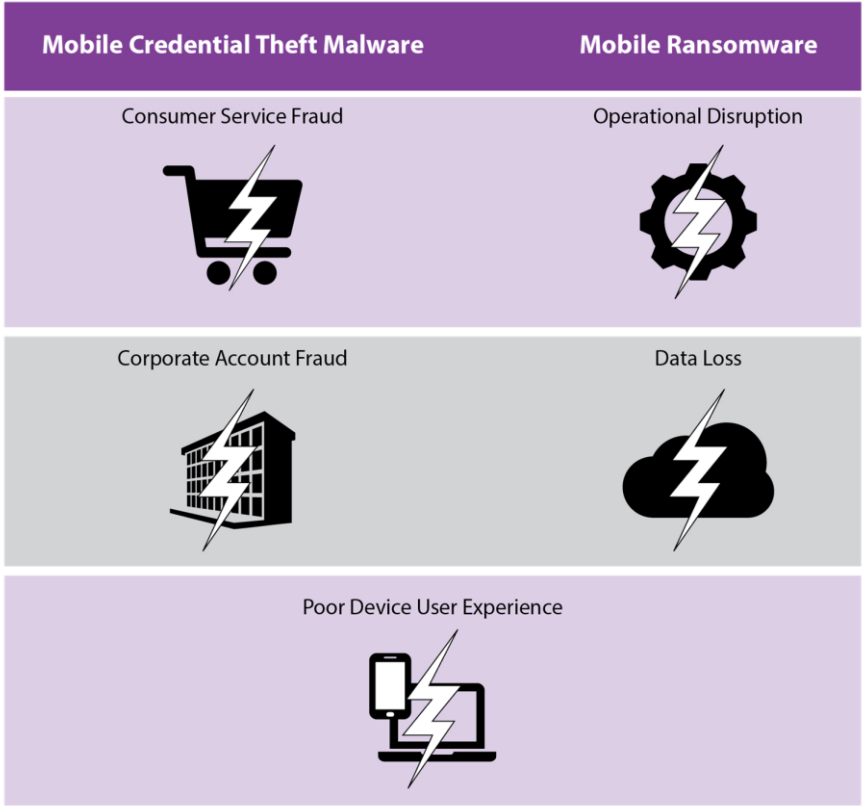
- Compromises user accounts with online banking and other services



Mobile Ransomware

- Blocks access or functionality, demands ransom to restore

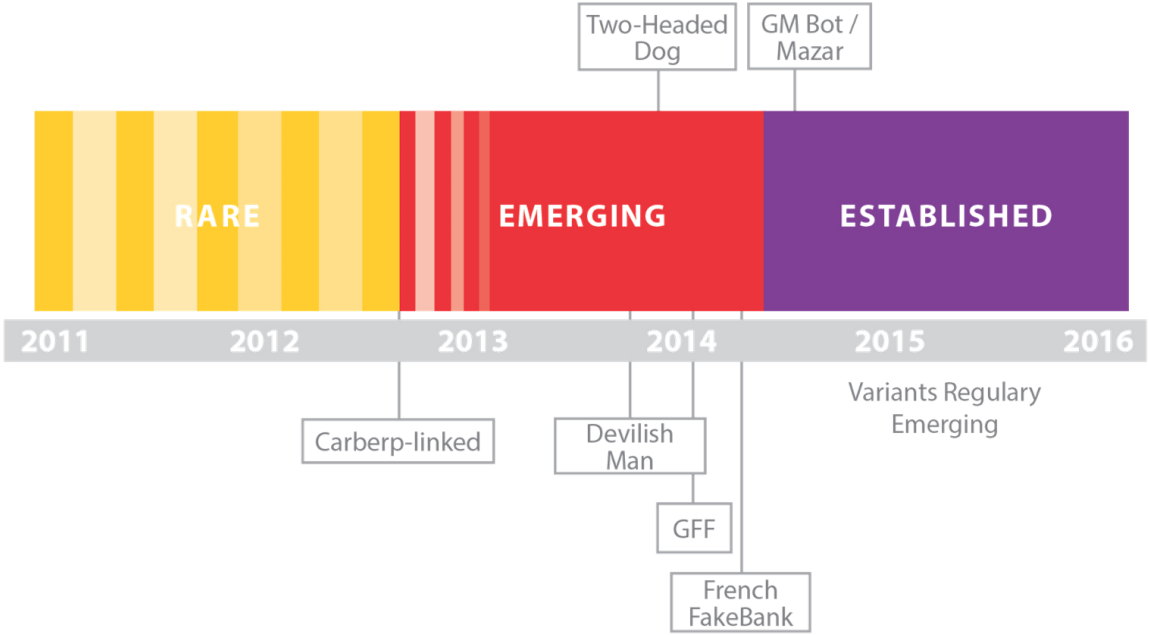
Introduction | Focus



- Why this focus?
  - Recent emergence
  - Rapid maturation
  - Significant threats

Mobile Credential Theft Malware

Credential Theft | History



Credential Theft | Current State

- **Campaigns affecting 100s – 1,000s of victims likely regular**
- Market leaders observable; competitors regularly emerge
- Target increasingly numerous banks & other organizations in multiple regions
- Compromises multiple authentication factors simultaneously
- Infects Android devices

Credential Theft | Injects

Windows malware "injects"

- Modify victim's experience of online service or interact with service
- Emerged following online banking security enhancements
- Diverse implementations created: circumvent MFA, record or modify displayed data, automate transfers…

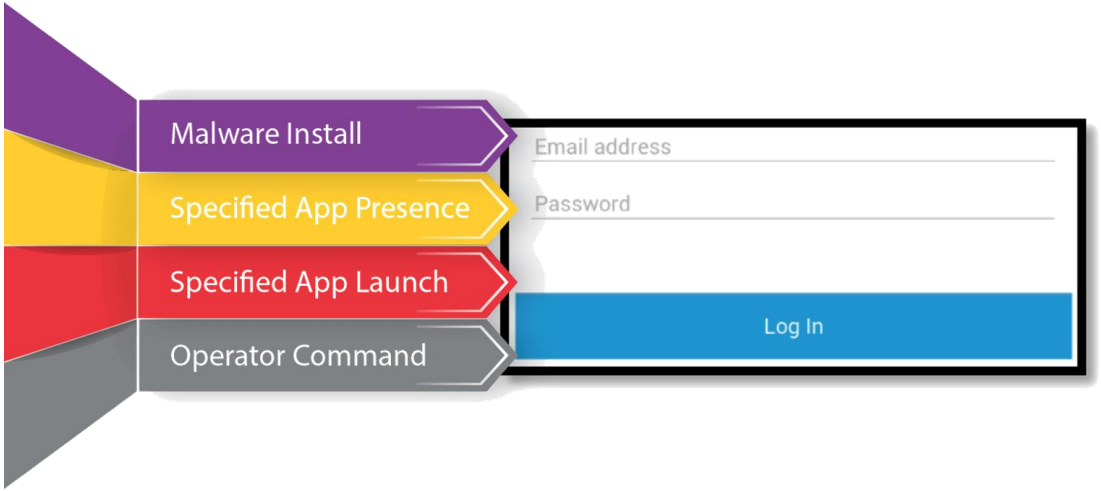
Android malware "injects"

- Modify victims' experience of device in general or specific app
- Emerged following mobile banking and payment apps
- Current implementation is primarily credential solicitation w/ other features used for MFA circumvention

Credential Theft | Case Study

Mazar: Latest Tool from Established Developer

- Credential theft / “injects”
  - Overlay legitimate app or standalone window
  - Multiple triggers

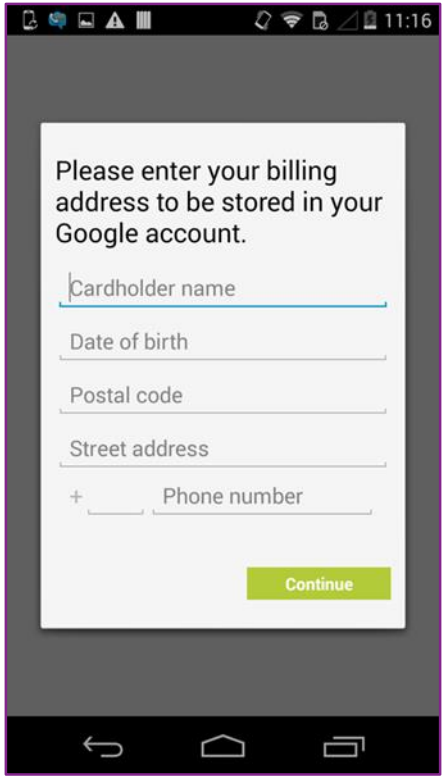


Credential Theft | Case Study

- Identified targets
  - **Services:** Online banking, payment cards, eCommerce, social media, communications
  - **Regions:** North America, Europe, Asia-Pacific
- Additional targets likely resulting from on-demand development efforts

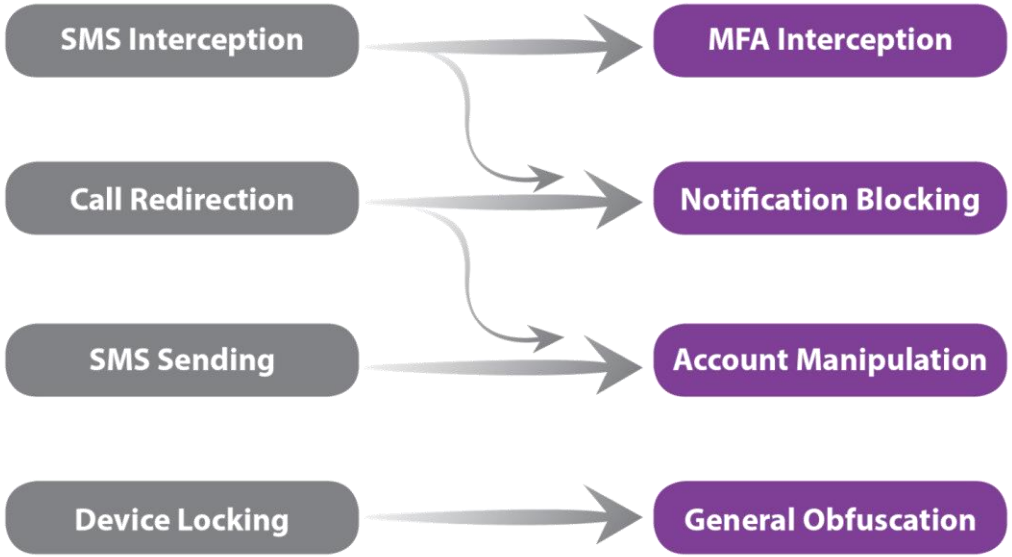
Credential Theft | Case Study

- Data gathered
  - **Online Banking:** Username, Password, MFA information
  - **Payment Card:** Number, Expiration, CVV, Name, PIN, 3-D Secure
  - **eCommerce:** Username, Password

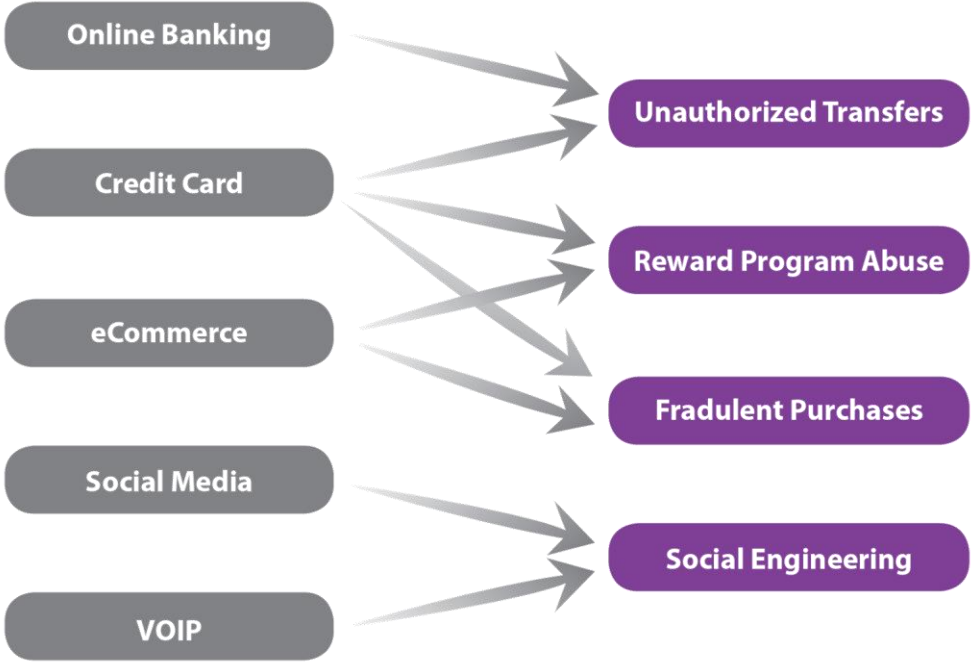


Credential Theft | Case Study

- Additional compromise vectors

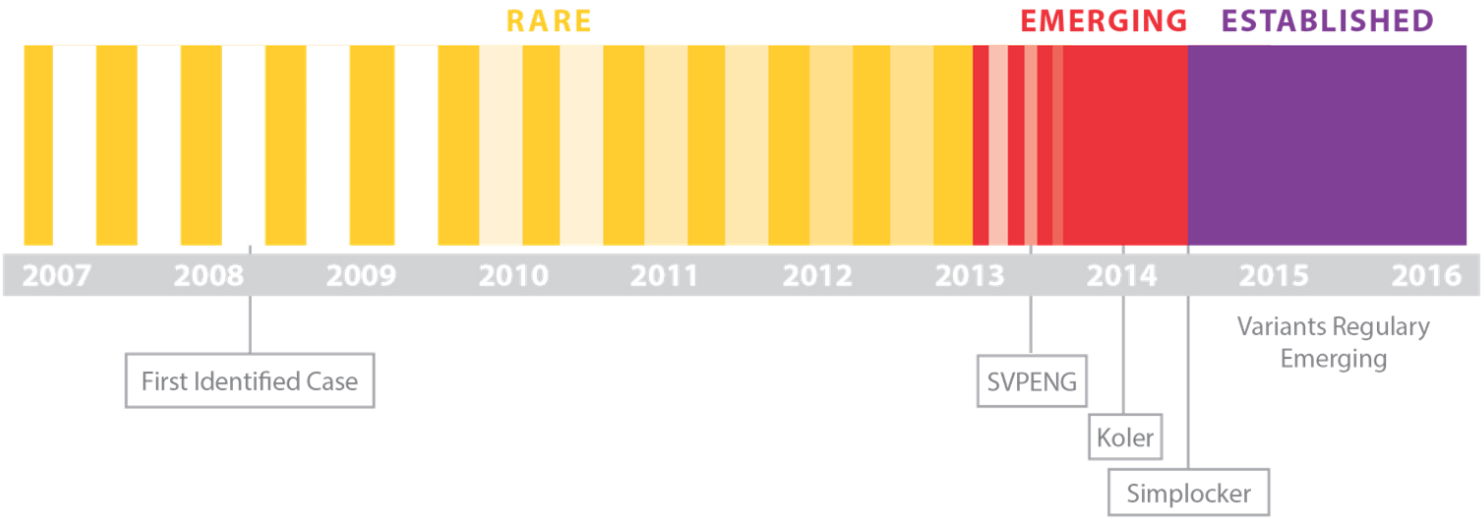


Credential Theft | Monetization



Mobile Ransomware

Ransomware | History

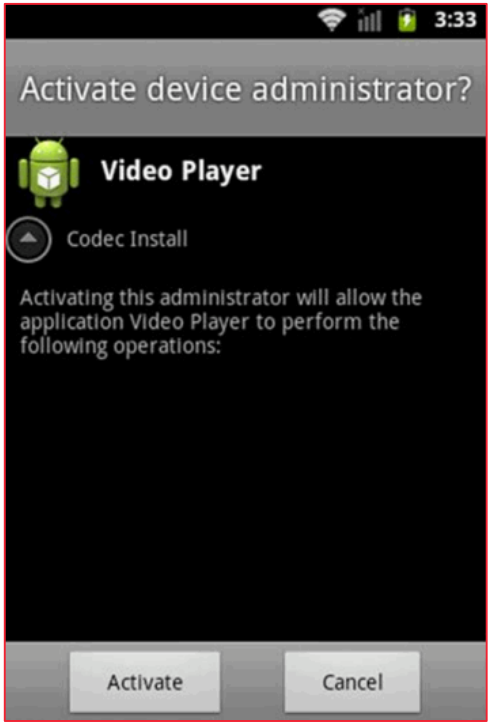


Ransomware| Current State

- **Accounts for large share of recent mobile infections**
- Primarily block device functionality; some encryption
- Linked to affiliate programs in eCrime marketplace
- Victims selected by country; increasingly global problem
- Primarily infects Android devices
  - Similar tactics applied to iOS through non-malware tools

Ransomware| Case Study

- **Simplocker:** First identified mobile ransomware to encrypt victims' files
- Distribution
  - Disguised as legitimate applications, often adult-themed
  - Hosted on fake Google Play sites



Ransomware| Case Study

- Extortive Behavior
  - Displays locked-device warning
  - Encrypts files on SD card: images, videos, documents
- Other Features
  - Collects device information, likely for campaign management
  - Jabber/XMPP-based C&C

Ransomware | Monetization

- Estimated average ransom amounts: $300 to $500 per victim device
- Commercial ransomware kits and services enable campaign operators to customize ransom amounts
- Victims forced to contribute to laundering process via payment in easily-handled currency

Outlook

Outlook | Credential Theft

- Geographic and sector scope of targeted services to expand
- Likely development focus: manipulating legitimate apps
  - **Interact** with specific apps
  - **Steal credentials** users enter legitimately
  - **Modify** app behavior

CREDENTIALS

Outlook | Ransomware

- Effects likely to remain focused on blocking functionality
  - Encryption of uncertain value
- Tools moving into commoditization stage → potentially rapid growth in distribution and use

Outlook | Cyber Criminal Mobile Malware

- Capabilities increasingly mirror conventional computer malware
- Increasing specialization leading to growing incidents
- Effective distribution tactics to be a focus
- Device targeting to expand slowly
- Conflict over maximizing malware functions and utility
  - **Pros:** Greatest benefit from overcoming installation challenges
  - **Cons:** Increased support difficulty and likelihood of remediation

Application

Application

- **Maintain mobile device replacement capability or workaround** to avoid productivity and accessibility disruptions
- **Ensure regular OS updates** to maintain security posture
- **Develop mobile device investigation capability** to assess incidents
- **Avoid isolated data on mobile devices** to limit impact of functionality loss
- **Achieve standalone, service-side fraud detection measures** to address account compromise without discernable client-side anomalies

Questions?