Club de la sécurité de l'information français

Panorama de la cybercriminalité année 2016

Paris, 11 janvier 2017

Evénement organisé avec le soutien de nos sponsors

Club de la sécurité de l'information français

CLUSIF

Malware et smarphones

Adrien PETIT
Team Manager Cyber Threat Intelligence – CEIS

Principaux OS ciblés

- Android, cible favorite des cybercriminels
  - Rappel : environ 900 000 nouvelles souches malveillantes détectées en 2015
  - Tendance confirmée en 2016
  - Principaux malwares
    - 07/2016 : rootkit **HummingBad**
    - 12/2016 : **Gooligan**, piratage du compte Google (et applications connexes) + activités de fraude
    - De plus en plus de ransomwares

Principaux OS ciblés

- iOS peu impacté
  - 03/2016 : **AceDeceiver** s'attaque au système de DRM « FairPlay »
  - 08/2016 : malware **Pegasus** d'origine étatique : 3 exploits zero-day + nombreuses fonctions liées à la surveillance

- 2 raisons peuvent expliquer cette différence
  - Répartition des terminaux : 84% des ventes au premier trimestre 2016 sous Android (17% sous iOS)
  - Apple Store : fort niveau de contrôle sur le développement et la distribution des applications

Focus sur le malware Mazar

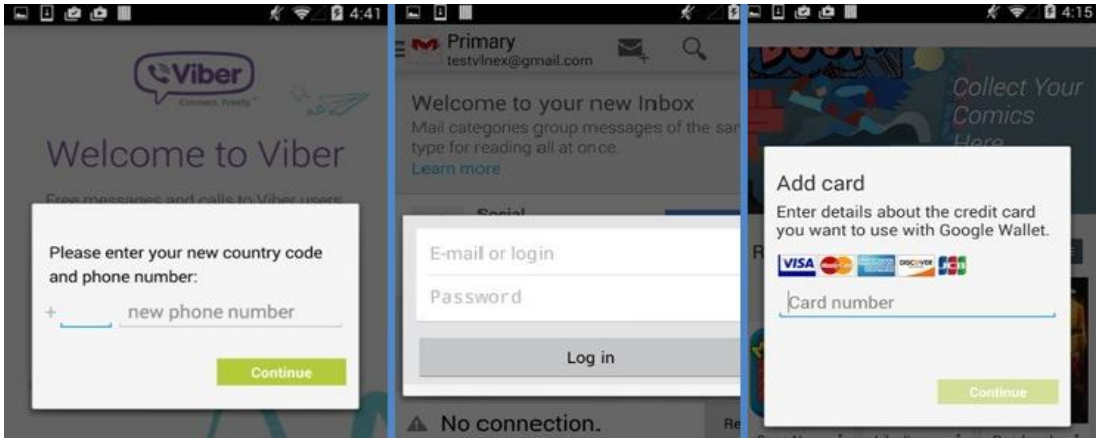
- Début 2016 : vague de cyberattaques liées au malware **Mazar** possédant des fonctionnalités avancées :
  - Surveillance et contrôle total du terminal (via une backdoor)
  - Envoi de SMS à des numéros surtaxés
  - Interception des SMS (notamment mécanismes 2FA)
  - Mise hors service du terminal
  - Coupure du son et de la vibration
  - Blocage des anti-virus
  - Etc.

→ Vendu sous le nom **GM Android VBV Grabber Bot** sur les forums underground russophones depuis octobre 2014

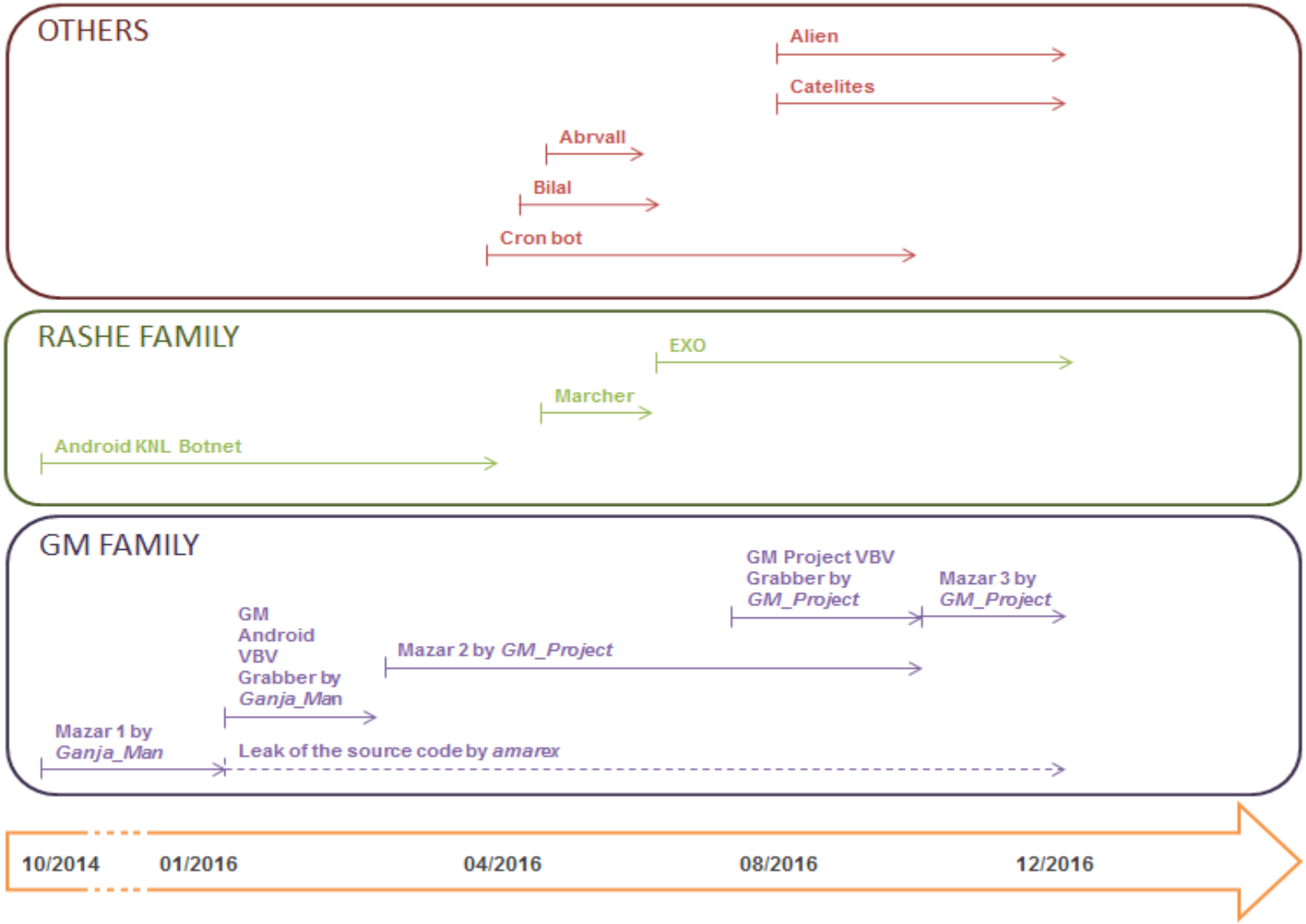
Focus sur le malware Acecard

- En parallèle son créateur Ganja_Man développa une nouvelle version baptisée **VBV Card Grabber** et **Acecard** par Kaspersky

→ **Généralisation** de la fonctionnalité de **App Injects**.
Superposition des injections par-dessus un grand nombre d'applications comme Gmail, Facebook, Skype, WhatsApp, Instagram, Paypal, Twitter, Google Play, Google Musique, ou encore les applications bancaires.



Timeline des malwares Android underground



Autres malwares Android

- De nombreux malwares sophistiqués tout au long de l'année 2016
  - **Android KNL** proposé par Rashe, concurrent historique de *Ganja_Man* depuis 2014. Nouvelle version appelée **Marcher**
  - **Bilal** : fonctionnalités peu nombreuses mais grande furtivité
  - **Cron bot** : double version Android (APK) et Windows (EXE)

- Suprématie des malwares historiques
  - **Exo Android Bot**
  - **Mazar 3**

→ Grabbing de cartes bancaires et listes de contacts dans les applis

État des lieux en décembre 2016

Exo Android Bot

- Successeur d'**Android KNL** et **Marcher**
- Vers 7.1.19 d'Android
- MAJ hebdomadaire
- Disponible seulement à la location : 750$ par semaine // 2400$ par mois
- Ne donne plus trop de caractéristiques techniques
- un service de loader Android

Mazar 3

- Vendu par GM_Project
- Opérationnel jusqu'à la version 6 d'Android
- **Grabbing de cartes bancaires et listes de contacts dans les applis**
- HTML injects
- Toujours App Injects
- Spam par SMS
- 2500 dollars (apk). Prix descend jusqu'au 01/12 à 999 dollars : plein d'acheteurs avec avis positifs

Une nouvelle typologie d'acteurs

- Développement de shops orientés App Injects
  - Vendeurs spécialisés comme *Kaktys* et *Candyman*
  - Applications bancaires dans un 1er temps
  - Extension à des applications plus « généralistes »
  - 250$/inject + Développement en 1 semaine

Diffusion des malwares

- SMS avec un lien malveillant
- Sous la forme de vraies/fausses applications (jeux d'argent, etc.)
  - Via Google Play
  - APK disponibles sur des sites extérieurs

Sources (1/3)

- McAfee Labs 2017 Threats Predictions
  http://www.mcafee.com/us/resources/reports/rp-threats-predictions-2017.pdf

- From HummingBad to Worse: New In-Depth Details and Analysis of the HummingBad Android Malware Campaign
  http://blog.checkpoint.com/2016/07/01/from-hummingbad-to-worse-new-in-depth-details-and-analysis-of-the-hummingbad-andriod-malware-campaign/

- More Than 1 Million Google Accounts Breached by Gooligan
  http://blog.checkpoint.com/2016/11/30/1-million-google-accounts-breached-gooligan/

Sources (2/3)

- AceDeceiver: First iOS Trojan Exploiting Apple DRM Design Flaws to Infect Any iOS Device
  http://researchcenter.paloaltonetworks.com/2016/03/acedeceiver-first-ios-trojan-exploiting-apple-drm-design-flaws-to-infect-any-ios-device/

- The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender
  https://citizenlab.org/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

- Gartner Says Worldwide Smartphone Sales Grew 3.9 Percent in First Quarter of 2016
  http://www.gartner.com/newsroom/id/3323017

Sources (3/3)

- Security Alert: Mazar BOT Spotted in Active Attacks – the Android Malware That Can Erase Your Phone https://heimdalsecurity.com/blog/security-alert-mazar-bot-active-attacks-android-malware/

- Android trump card: Acecard https://blog.kaspersky.com/acecard-android-trojan/11368/

- The evolution of Acecard https://securelist.com/blog/research/73777/the-evolution-of-acecard/