Fintech周りの
セキュリティ脅威とその対策の検討

佐々木　潤世
セールスエンジニアリング本部

2017/07/10

SOPHOS

Fintech周りサイバー脅威（端末を中心に）

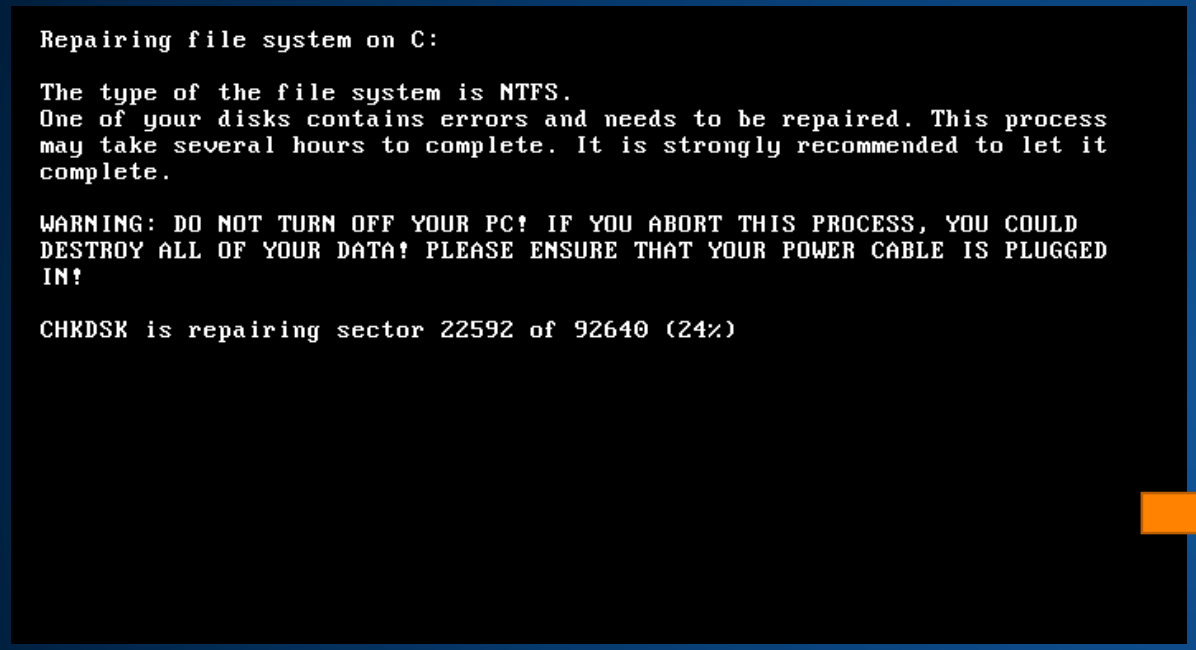
- 不正送金マルウエア
  - Dreambot (日本をターゲットにしたマルウエア)
  - Gozi(Ursnif)

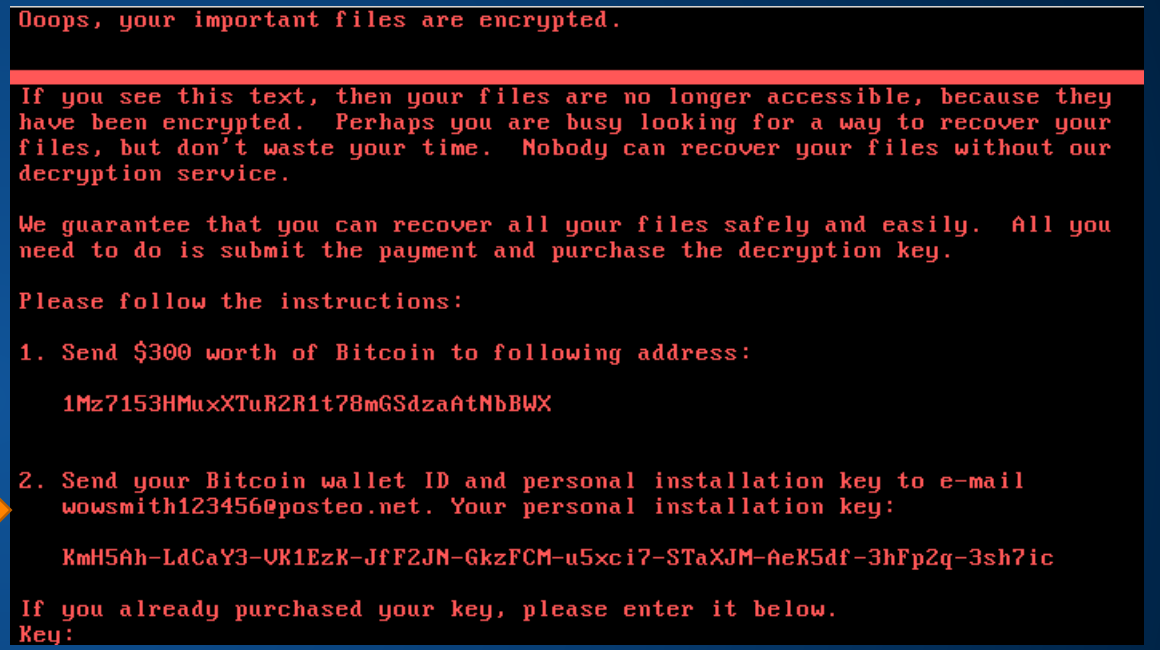
- ランサムウエア
  - Petya(NotPetya)
    - ウクライナ、ロシア、EU諸国、USA、等
    - 政府、金融、交通、放送、電力、通信、医療
    - POS、Kiosk端末も被害
  - WannaCry
    - アジア、EUが被害。
    - 製造、医療、交通、政府

WannaCry

社会インフラに対して
大きな影響を与えている

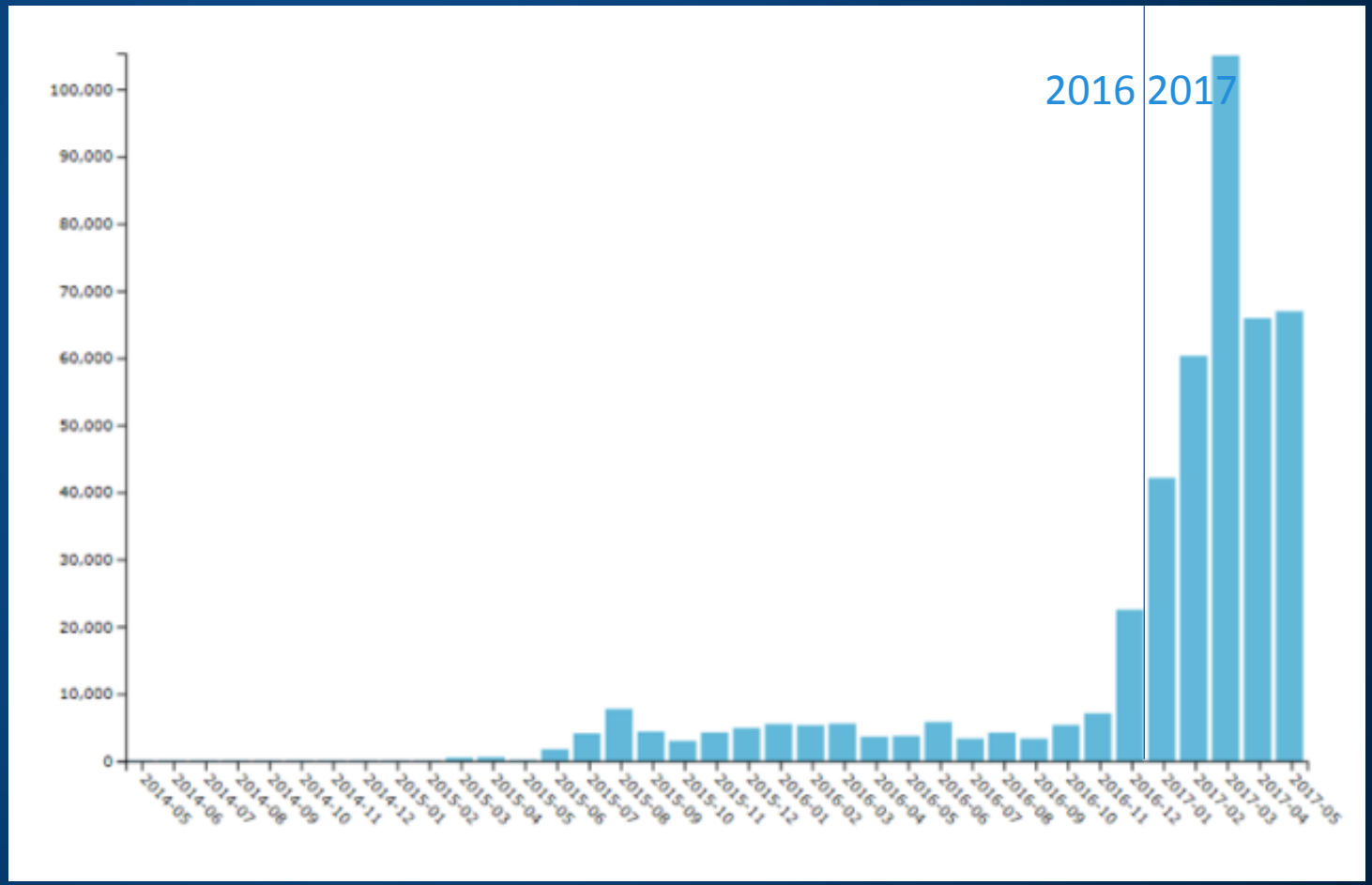
Petya(NotPetya) 強制リブート後…





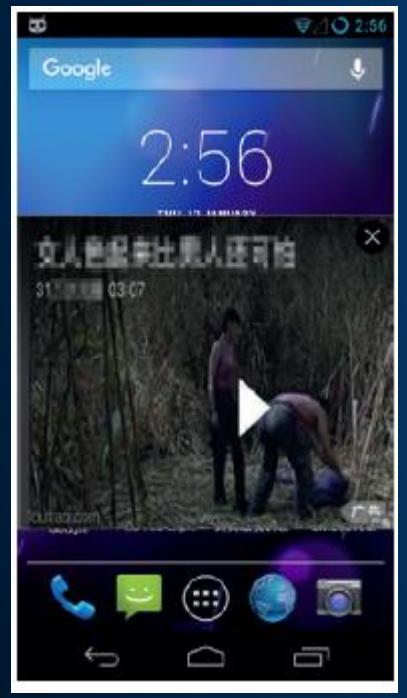
ランサムウエア on Android

- 観測上2016の後半から急激に増加



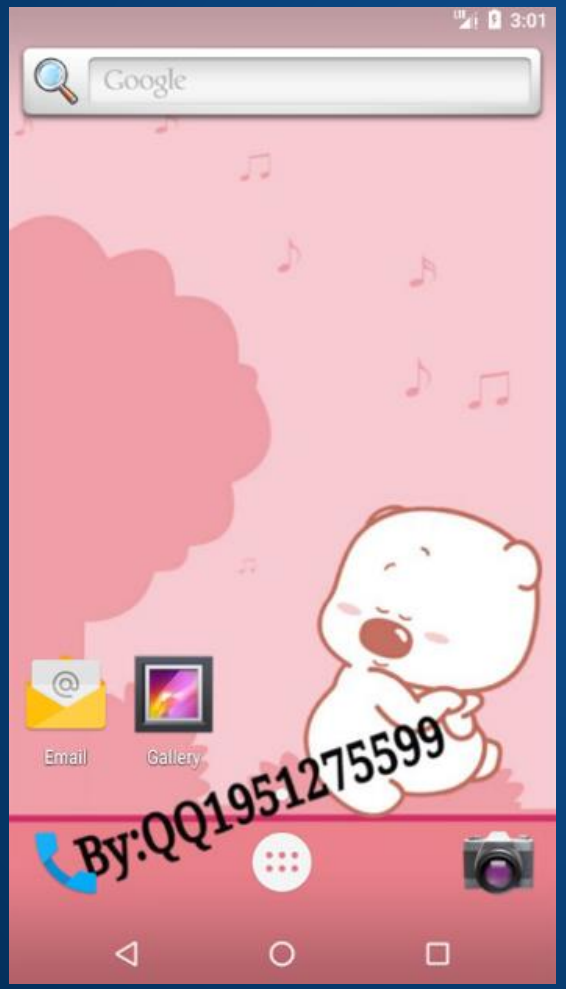
PornClk

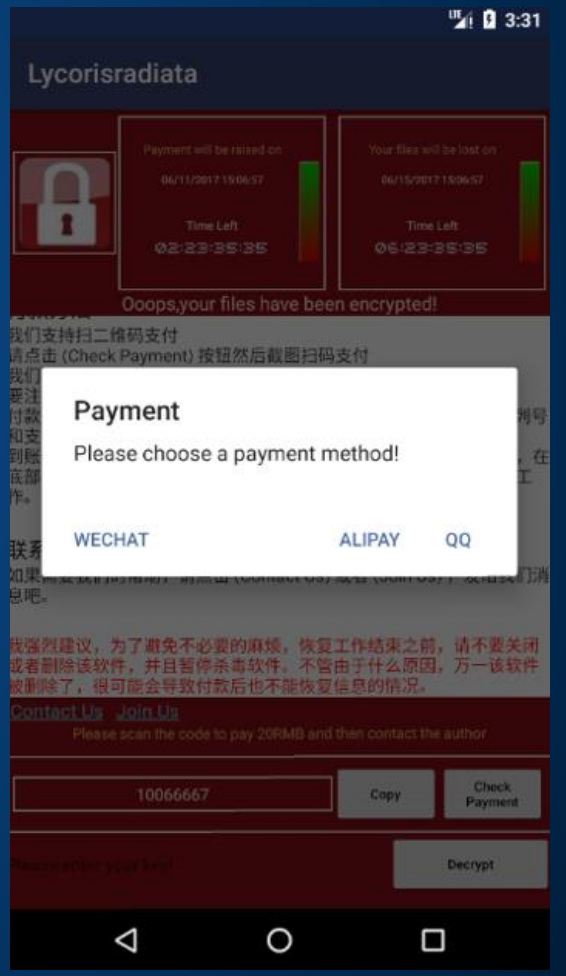
- Androidをターゲットにしたランサムウエア？
  - 暗号化するわけではないが、操作を制限することで身代金を要求。




Fake apps of “King of Glory”:王者栄耀

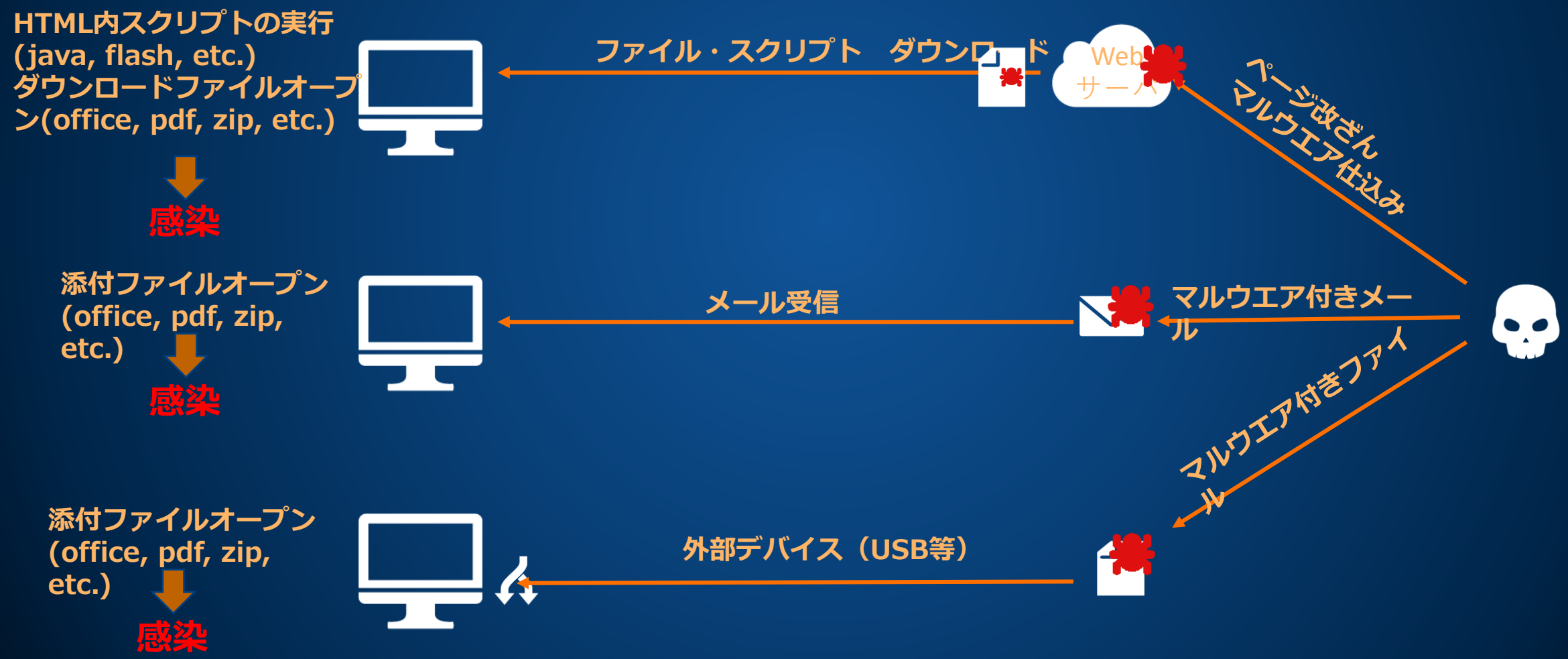
- アンドロイド版ランサムウエア



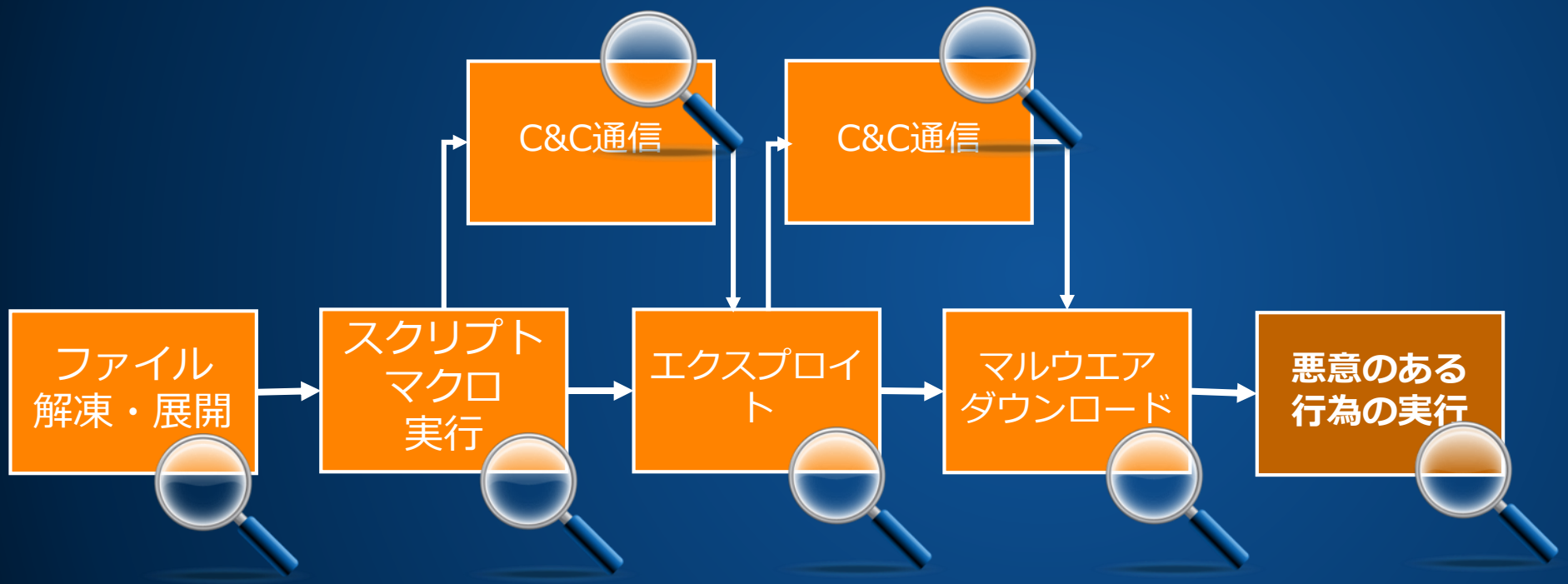


マルウエアの侵入経路

- 3つのパターン



侵入後手順



機密データ窃取

クレデンシャル
窃取

ファイル暗号化

ファイル改ざん

マルウエア（悪意のあるプロセス行動）

- いくつかの不正行為はあるが、根本的に、最初におこなうは

- 権限の奪取
  - これができれば、あとはなんでもできる。

クレデンシャル窃取

  - そこをいかにして守るか

Fintech周りのサイバー脅威

- セキュリティベンダーからのソリューション
  - ソフォスも含め、多種多様なソリューションを提供している。
  - 悪意のあるハッカーやシンディケートがあらゆる手段で、情報コンテンツを窃取することや改ざんすることを日々開発している。
  - セキュリティベンダーは、その都度、対応する盾を提供している。

  - 多層防御がデフォルト

  - それらの防御策を、コンシューマや無人・簡易端末に適用できるのか？

コンシューマに情報リテラシーを求められるか (PC，スマートフォン対策)

- 多様・多数の顧客が個人情報管理を任せられる？
  - ゲームアプリとFintechアプリが共存。
    - 野良アプリも使っている可能性がある。
    - 金融サービス側が他のアプリの使用の停止を求めることはできない。
  - 巧妙化するソーシャルエンジニアリング
    - 簡単に野良アプリに特権を与えてしまう可能性がある。
    - Fintechアプリにもアクセスできる？アプリ管轄内のファイル、メモリを参照できる？
- Fintechアプリもなんらかの防御機構が求められる。
  - 情報の保管場所と内容の機密化
    - 取引情報の暗号化
    - 暗号化鍵の機密化
    - クレデンシャル情報の機密化
  - でも、OSレベルやブラウザレベルの脆弱性があると、破られる可能性がある。

IoTデバイスはセキュアにできるのか

- IoTデバイスの存在
  - ATM、Kiosk端末、POS端末
- セキュアな形で通信は確保されている（筈）
  - L1/2での専用線接続
  - VPNでの接続
- 物理的な保護は
  - IoTデバイス自体に対する保護が保障されるか？
  - USB, Ethernet, Bluetooth, Wifi
    - 直接マルウエアを仕込むこともありうる。

サービス提供者側でできること

- ユーザに提供するセキュアなアプリを提供すること
  - しかし、ユーザの利便性も考えなければ、、、
  - FIDO認証
    - 認証機構の選択に柔軟性
    - ２FA（MFA)
  - でも、最後はアプリ側がどのように実装するかが重要。

ディスカッションテーマ

- 目指すは、、、
  - OSがハックされても、アプリ上で動作するクレデンシャルは窃取されない？
  - クレデンシャルがハックされそうなことやハックされたことを検知するシステムが構築できないか。。

SOPHOS

Security made simple.