

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）

- 不正送金マルウェア
 - Dreambot (日本をターゲットにしたマルウェア)
 - Gozi(Ursnif)
- ランサムウェア
 - 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…

Repairing file system on C:

The type of the file system is NTFS.
One of your disks contains errors and needs to be repaired. This process may take several hours to complete. It is strongly recommended to let it complete.

WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED IN!

CHKDSK is repairing sector 22592 of 92640 (24%)



Oops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.

We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send \$300 worth of Bitcoin to following address:

1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWx

2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:

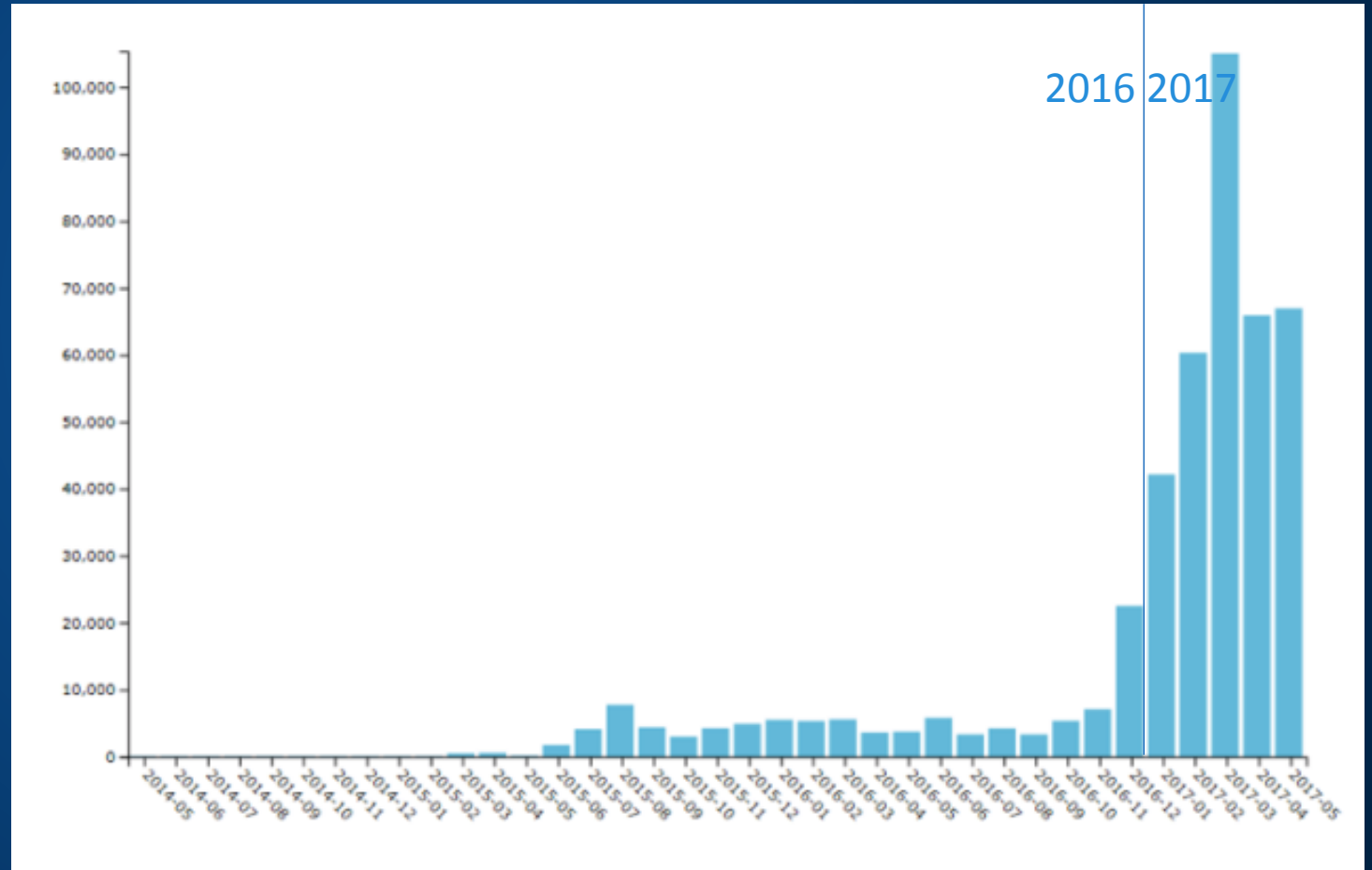
KmH5Ah-LdCaY3-UK1EzK-Jff2JN-GkzFCM-u5xc i7-STaXJM-AeK5df-3hFp2q-3sh7ic

If you already purchased your key, please enter it below.

Key:

ランサムウェア on Android

- 観測上2016の後半から急激に増加



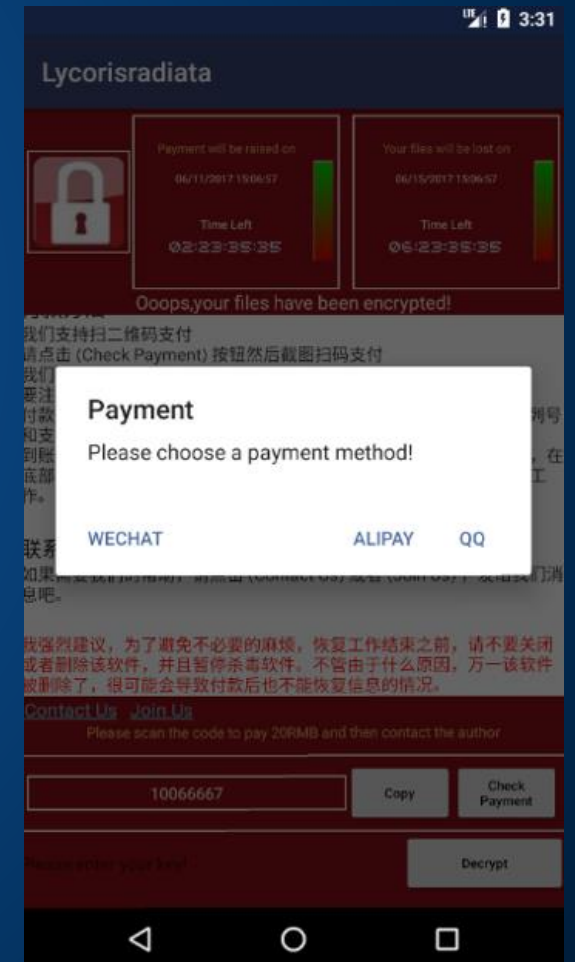
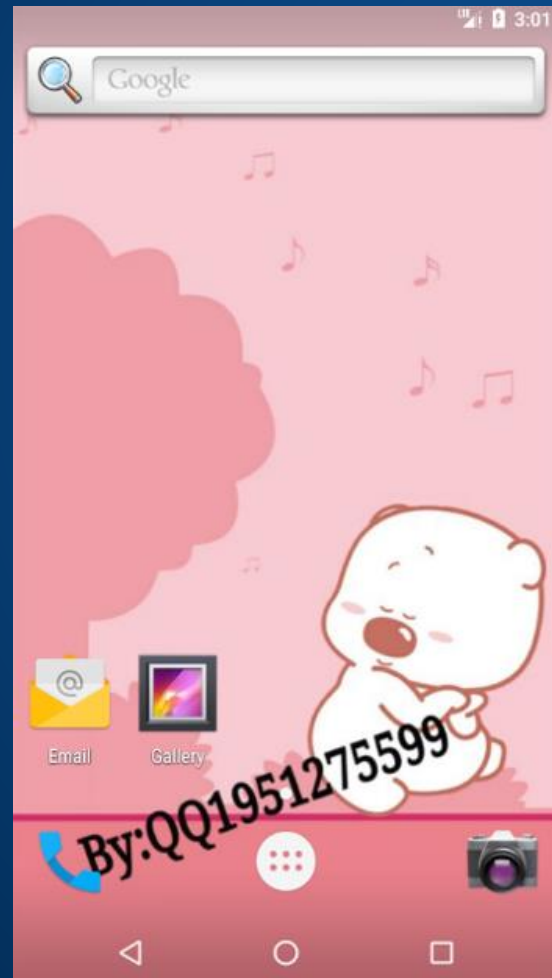
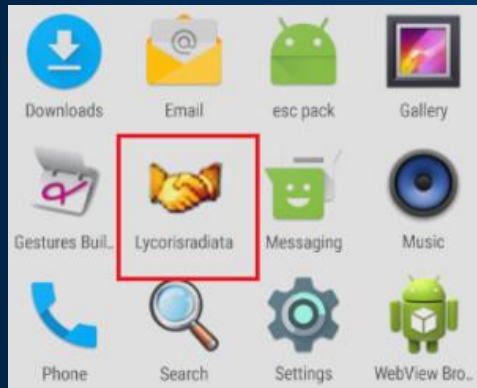
PornClk

- Androidをターゲットにしたランサムウェア？
 - 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”:王者荣耀

- アンドロイド版ランサムウェア



マルウェアの侵入経路

- 3つのパターン

HTML内スクリプトの実行
(java, flash, etc.)
ダウンロードファイルオープン
(office, pdf, zip, etc.)

感染

添付ファイルオープン
(office, pdf, zip,
etc.)

感染

添付ファイルオープン
(office, pdf, zip,
etc.)

感染



ファイル・スクリプト ダウンロード



Web
サーバ

ページ改ざん
マルウェア仕込み

メール受信



マルウェア付きメール

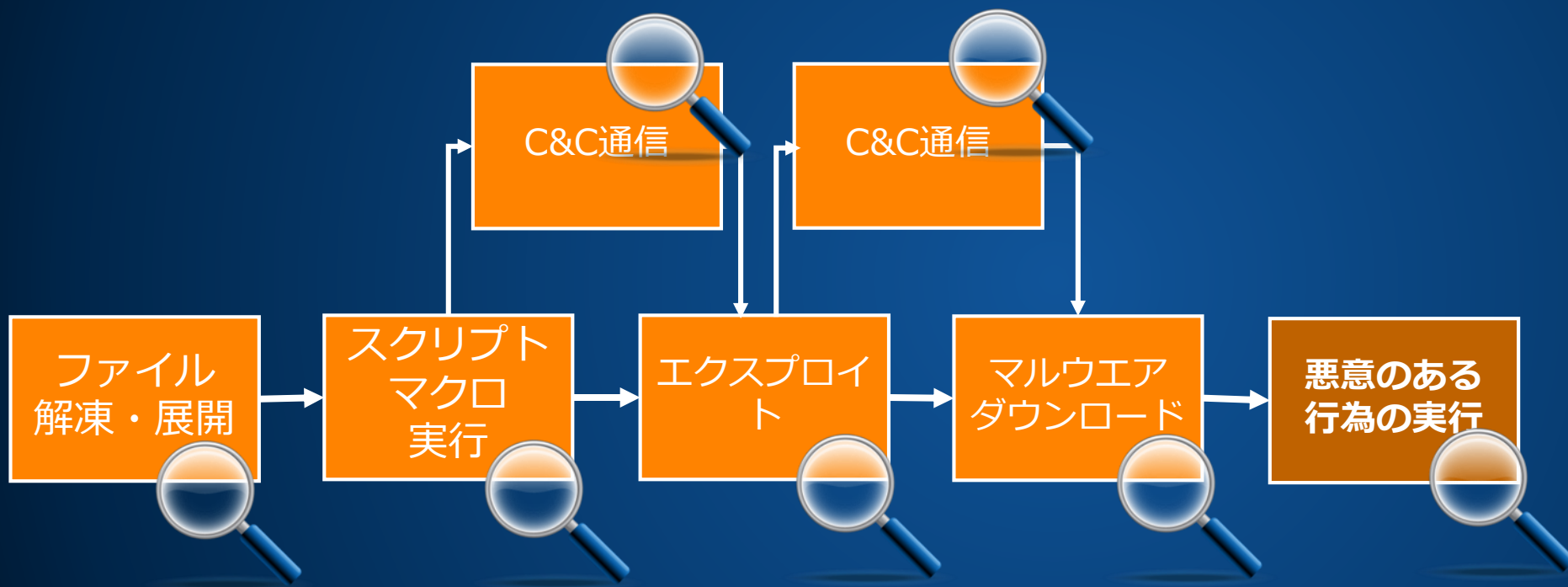


外部デバイス (USB等)



マルウェア付きファイル

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

マルウェア（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
 - 直接マルウェ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.