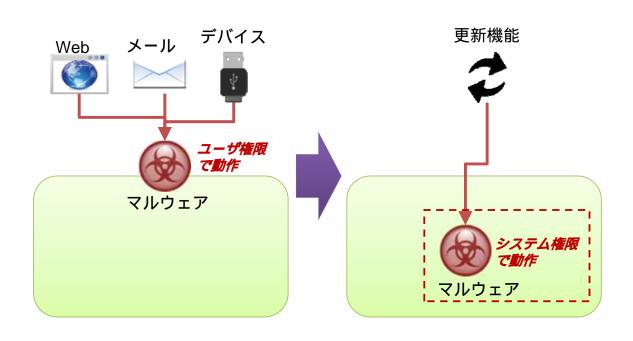
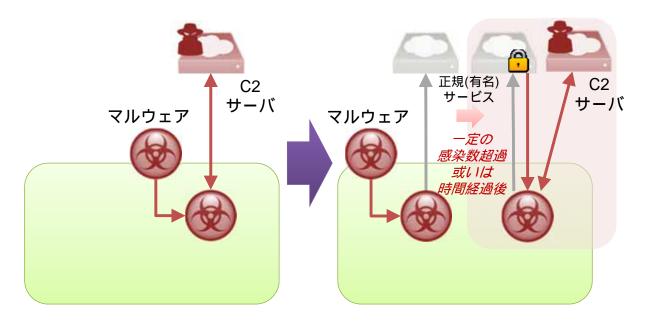
「攻めのデジタル・フォレンジック」が 必然的に求められる状況変化

2017年 12月 11日 名和 利男

更新機能を利用するマルウェア感染



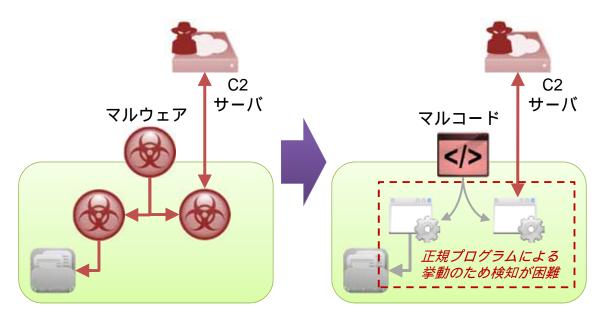
<u>正規(有名)サービスを(時間差で)踏み台</u>にするC2通信



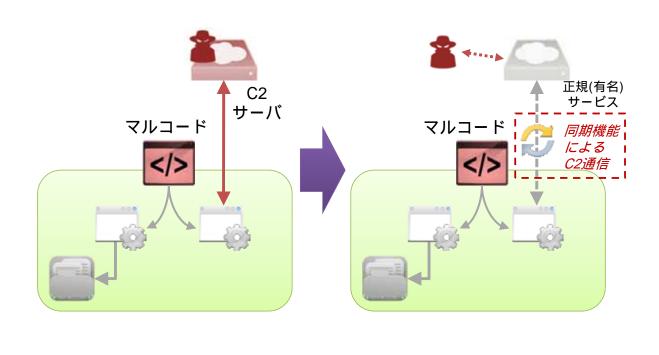
Copyright © 2017 Toshio Nawa All rights reserved.

3

スクリプト実行環境を利用した<u>正規プログラム</u>による挙動



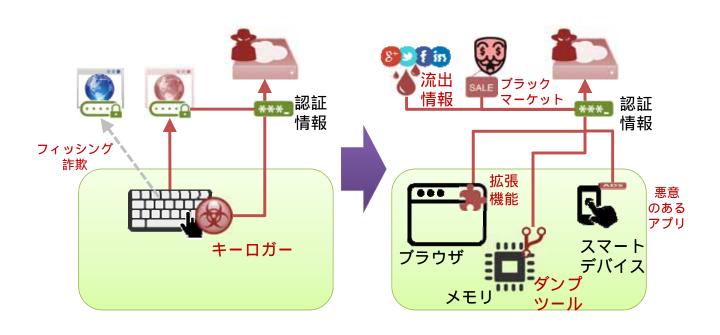
正規(有名)サービスの同期機能を利用するC2通信



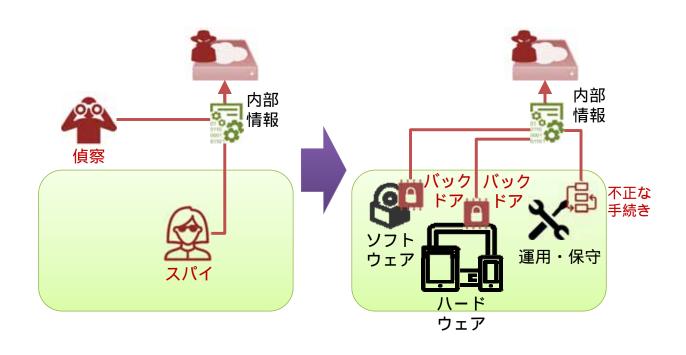
Copyright © 2017 Toshio Nawa All rights reserved.

5

様々な対象から**調達・窃取可能な認証情報**の悪用



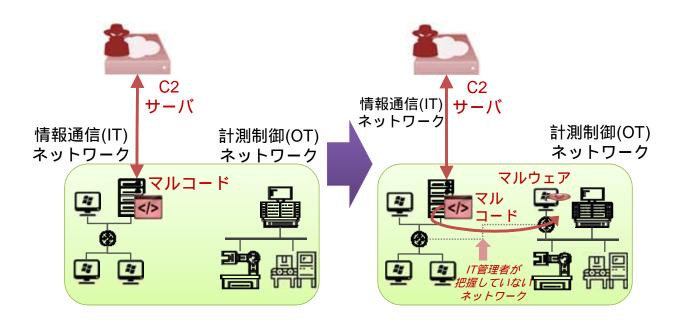
敵対国のソフトウェアやプロダクトからのデータ流出



Copyright © 2017 Toshio Nawa All rights reserved.

7

機械設備のPCに対するマルウェア感染



本資料に関する連絡先

名和 利男 (Toshio NAWA)

Email: toshio@nawa.to

SNS: about.nawa.to

Tel: 03-3242-8700 (サイバーディフェンス研究所)

Copyright © 2017 Toshio Nawa All rights reserved.

9