サイバー攻撃の事後追跡不可能性とデジタル･フォレンジック

ネットエージェント株式会社
フォレンジックエバンジェリスト
松本 隆

本日の内容

①サイバー攻撃の事後追跡不可能性
・ネットワーク調査の事後追跡困難化
・マルウェアを取り巻く状況の変化

②次のデジタル･フォレンジック

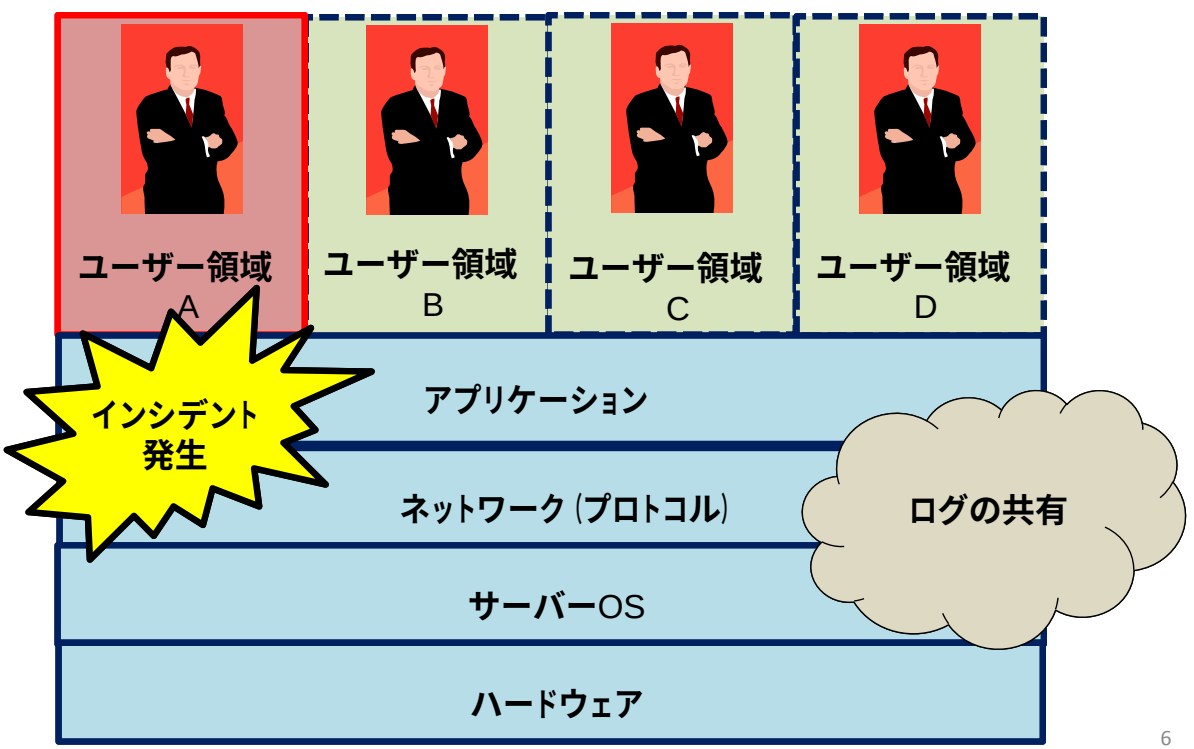
①サイバー攻撃の事後追跡不可能性
ネットワーク調査の事後追跡困難化

ネットワークの事後追跡困難化
※このページは非配布です

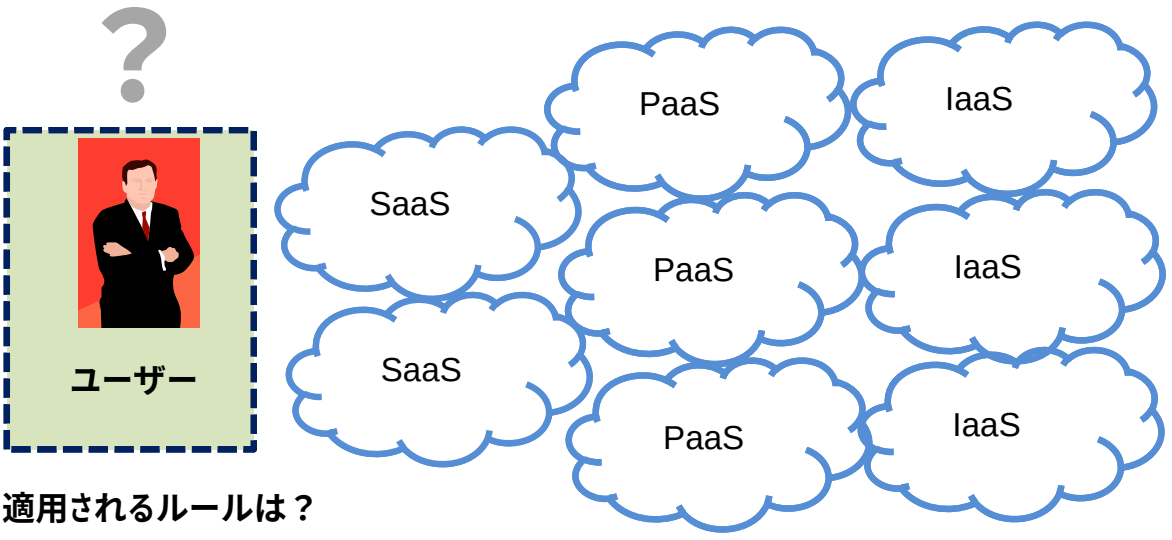
ネットワークの事後追跡困難化

- もともと事後追跡は苦手
  - 決定的な本人認証手段が存在しない
    - 本人認証は別の手段が必要
    - そもそも従来のネットワーク調査**だけ**では本人までつなげるのは困難（例：PC遠隔操作事件）
  - 流れているデータが何か分からない
    - 通信の暗号化が当たり前の時代
    - お手軽な通信の匿名化ツールの普及
    - 簡単に可能な通信の詐称、偽装
  - そもそも必要な履歴が残りにくい
    - 最新に「上書き」
    - 監査や調査目的でのログの保管に関する実質的な取り決めがない（内容、量、質）

ネットワークの事後追跡困難化
クラウド：ログの共有



ネットワークの事後追跡困難化
クラウドのサプライチェーン問題



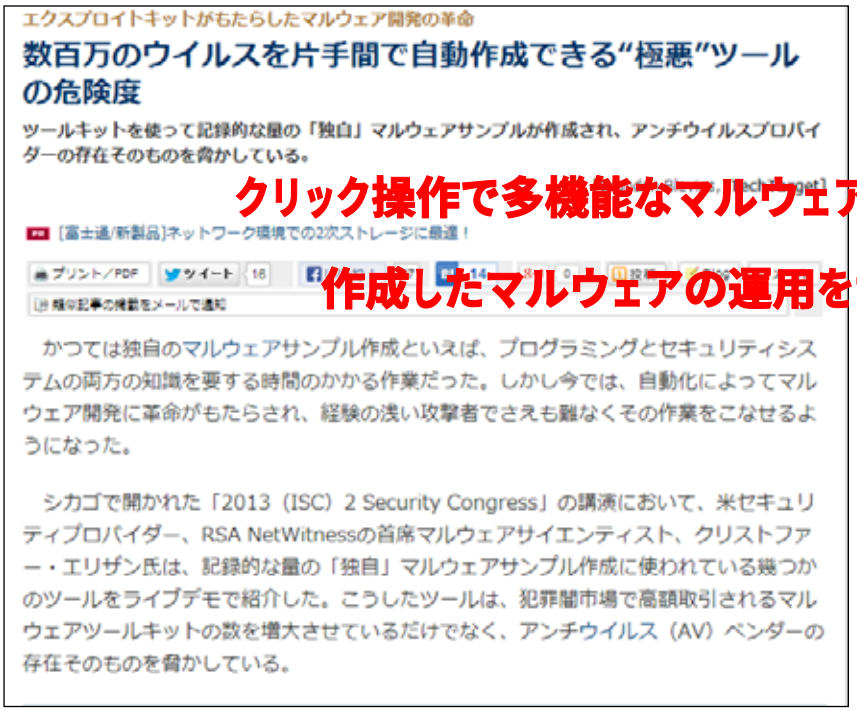
適用されるルールは？

契約はどうなってる？

ログは？

マルウェアを取り巻く状況の変化

マルウェア･ツールキットやエクスプロイトキットの台頭



エクスプロイトキットがもたらしたマルウェア開発の革命

数百万のウイルスを片手間で自動作成できる“極悪”ツールの危険度

ツールキットを使って記録的な量の「独自」マルウェアサンプルが作成され、アンチウイルスプロバイダーの存在そのものを脅かしている。

クリック操作で多機能なマルウェアが作成可能

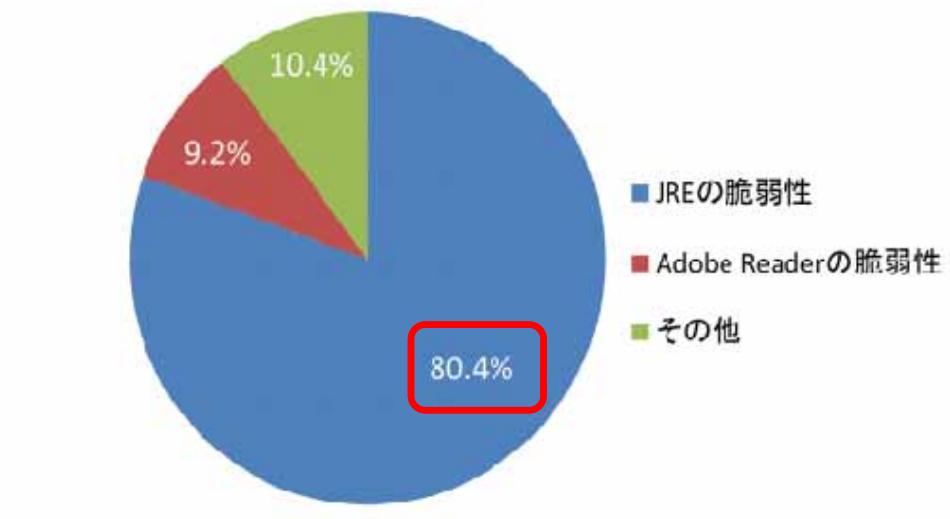
作成したマルウェアの運用をサポート

かつては独自のマルウェアサンプル作成といえば、プログラミングとセキュリティシステムの両方の知識を要する時間のかかる作業だった。しかし今では、自動化によってマルウェア開発に革命がもたらされ、経験の浅い攻撃者でさえも難なくその作業をこなせるようになった。

シカゴで開かれた「2013（ISC）2 Security Congress」の講演において、米セキュリティプロバイダー、RSA NetWitnessの首席マルウェアサイエンティスト、クリストファー・エリザン氏は、記録的な量の「独自」マルウェアサンプル作成に使われている幾つかのツールをライブデモで紹介した。こうしたツールは、犯罪闇市場で高額取引されるマルウェアツールキットの数を増大させているだけでなく、アンチウイルス（AV）ベンダーの存在そのものを脅かしている。

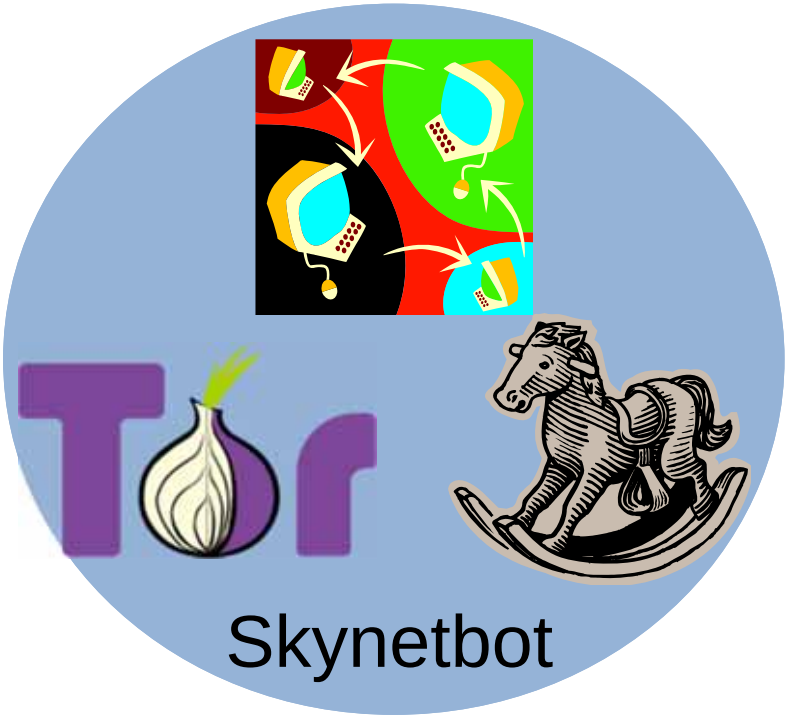
http://techtarget.itmedia.co.jp/tt/news/1311/08/news05.html

マルチプラットフォーム化
ドライブ･バイ･ダウンロード攻撃におけるOracle Java Runtime Environment(JRE)脆弱性の利用増加



2013年上半期 Tokyo SOC 情報分析レポート より

アンチフォレンジック：通信の匿名化
Skynetbot-マルウェアとボットネットとTorの融合



アンダーグラウンドコミュニティの変化：プロジェクト化
ある日のコミュニティの会話①
どうやってお金を稼ぐ？

how do you make money with this?

Mining bitcoins and exchange them into dollars. Selling banking, billing, credit card information to 3rd parties.

How much money in total have you made through this?

以下議論が続く・・・

目的の明確化

アンダーグラウンドコミュニティの変化：情報共有
ある日のコミュニティの会話②
ウイルススキャン製品のソース共有

Having the Kaspersky engine on my hand is sufficient (and I feel self-sufficient). But still, where are the source codes from Norton AV[redacted]

Well .... right here

https:[redacted]/norton%2[redacted]

thanks

情報共有

アンダーグラウンドコミュニティの変化：情報共有
ある日のコミュニティの会話③
競合マルウェアのリポジトリ共有

The package has everything, Carberp is one of many.

Uncompressed: 5.13 GB
Contain 31.511 files and 4.808 folders

Carberp is a particularly ugly modification of ZeuS clearly aiming the script kiddies audience.

Big bunch of commercial turd. End of story.

Don't write stupid opinions before download the file and examine the sources codes.
There is much to see, learn and get a little inspiration.

Bitcoinとマルウェア

http://arstechnica.com/security/2013/10/youre-infected-if-you-want-to-see-your-data-again-pay-us-300-in-bitcoins/

BitcoinのPaypalライクなサービスOnionbank

安全にBitcoinを交換するサービス

http://vk.com/topic-29387592_28983005

匿名化メールサービスTor Mailと アンダーグラウンド

メールをTorの技術で匿名化

http://tormail.org/

マルウェアを取り巻く状況の変化

- 多様化
  - マルウェア・ツールキットやエクスプロイトキットの台頭
  - マルチプラットフォーム化
  - アンチフォレンジック対応
- アンダーグラウンドコミュニティの変化
  - マルウェア開発のプロジェクト化
  - 情報共有
  - 進むアングラビジネスの匿名化

2　次のデジタル･フォレンジック

事後追跡不可能性～
なぜ事後追跡が不可能なのか

- 利用者本人まで繋がらない
- そもそも現状のプラットフォームが履歴を残す仕様ではない
- 事後対応の技術的限界
  - 仮想化、共有化、オープン化…
  - 攻撃手法の複雑化、高度化…
  - アングラコミュニティの自由度…

事後追跡可能性～
デジタル･フォレンジックが期待すること

- 利用者本人まで繋がるシステム
  - 本人認証の手段を組み込む
  - 既存の監視カメラのようなログとタイムラインを統合
- 現状のプラットフォームが残さない履歴を残す仕組みへ
  - ディスクに残らないマルウェアへの対応
  - 上書きされ消されていく履歴をすぐに利用可能な状態で保全

過渡期的な対応

- **事後対応の技術的限界**
  - リアルタイム･ライブ対応可能なプラットフォームや体制の構築
  - 証跡に関する規定の明確化
  - 自由な情報共有へ向けた取り組み

一歩先に進むために･･･

＜メモ＞