

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

- 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

次のデジタル・フォレンジック

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



3

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



4

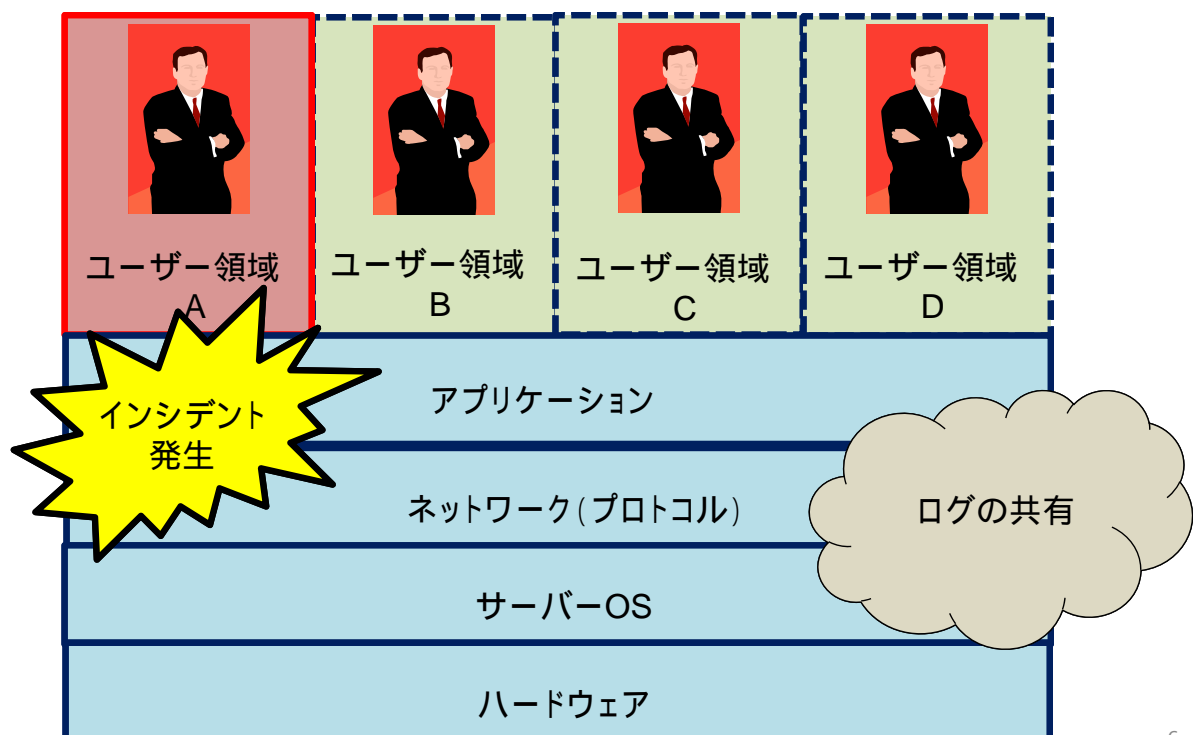
ネットワークの事後追跡困難化

• 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)

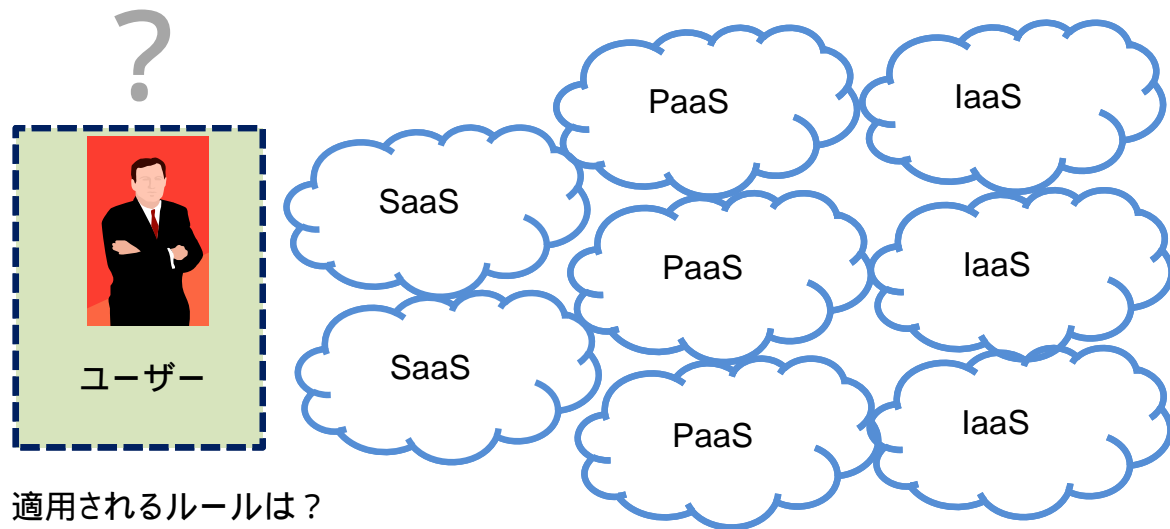
5

ネットワークの事後追跡困難化 クラウド:ログの共有



6

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？

7

マルウェアを取り巻く状況の変化



8

マルウェア・ツールキットや 익스プロイトキットの台頭

익스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。

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。

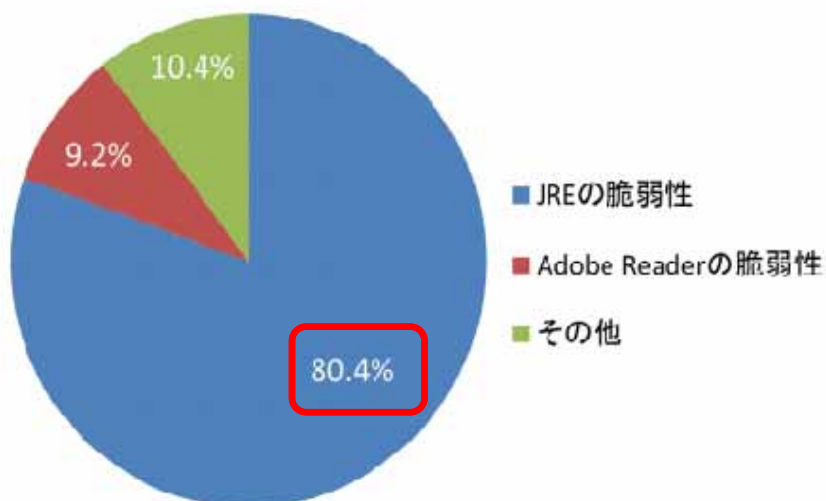
クリック操作で多機能なマルウェアが作成可能

作成したマルウェアの運用をサポート

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

9

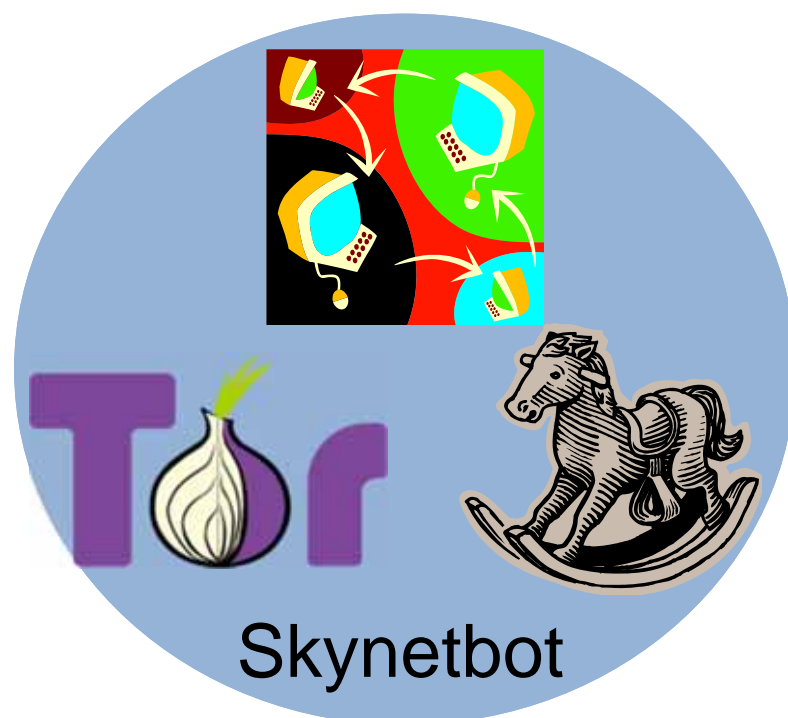
マルチプラットフォーム化 ドライブ・バイ・ダウンロード攻撃におけるOracle Java Runtime Environment(JRE)脆弱性の利用増加



2013年上半期 Tokyo SOC 情報分析レポートより

10

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



11

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
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

12

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 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? 😊

Well right here 😊

<https://.../norton%...>

thanks

情報
共有

13

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 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 😊

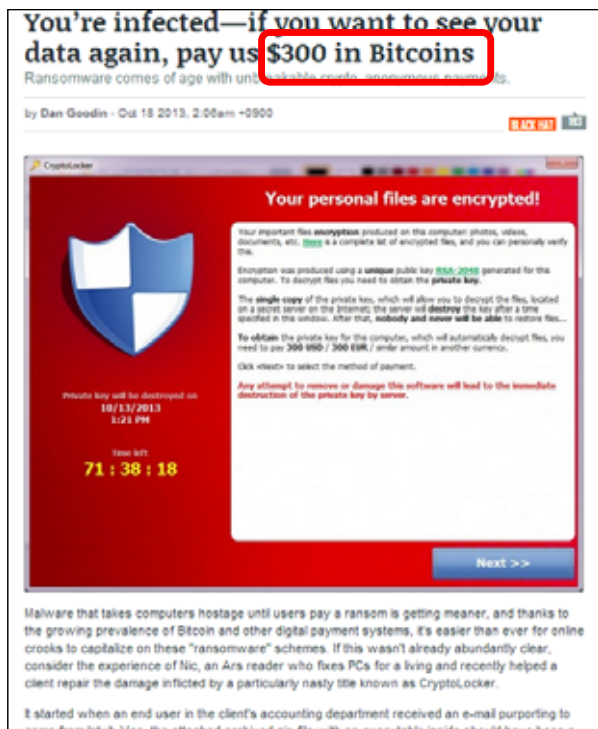
Carberp is a particularly ugly modification of Zeus clearly aiming the script kiddies audience.

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.

14

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/>

15

BitcoinのPaypalライクなサービスOnionbank

← All about Bitcoin, Mining, news Bitcoin sign up

Discussion board Discussion

Onion Bank emerged from the creator of Freedom Hosting

Rusiar Sevryanin

There are 2 posts in this discussion

 **Rusiar Sevryanin**

I decided today to go to your account at Freedom Hosting and on the main page, I saw a new ad. I'm not good at English, so a translator translated: It's been two years since the open enrollment of new hosting accounts Freedom Hosting has been closed and replaced by invitation only system that has been done to prevent the attacks of DDoS. I initially said will have the option to buy at a low price due to \$ 5 with bitcoins, but nothing came of it, mainly because there was no easy way for the adoption of bitcoins onion territory, without having to install bitcoin software. This gave me the idea that I should Create one place where merchants can easily sign up and take bitcoins on their onion territories. Onion I created a bank that was in the (slow) development for almost two years! Originally it was supposed to include an anonymous exchange between Liberty Reserve and Bitcoins, but since the closure of LR it is now only one place to bitcoin. One of the problems with the use of bitcoin on the Tor network is anonymous, with bitcoins is blockchall, which can link your buy or sell bitcoins on exchanges with sites that accept them in order to use their anonymity is required, the overall system wallet / laundry. Onion Bank does all this and more, the ability to accept and spend bitcoins anonymously. Using Onion Bank can accept bitcoins on my website, full automation is possible. You can also set a bond payment / donation for your site. Features include ... Business Services SCI / IPN. multiple identities under a single account. Produces a new bitcoin address for each transaction. Escrow. Laundry. Bank address <http://onionbank6fdaccy.onion/>

安全にBitcoinを交換するサービス

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

16

匿名化メールサービスTor Mailと アンダーグラウンド

Tor Mail

Tor Mail is a free anonymous email service provider

Tor Mail is a [Tor Hidden Service](#) that allows anyone to send and receive email anonymously.
This product is produced independently from the Tor® anonymity software and carries no guarantee from [The Tor Project](#) about quality, suitability or anything else.

For more information, or to sign up for your free @tormail.org account, which includes webmail, smtp, pop3, imap access.
Please visit our Tor hidden service at <http://shh-willagvaawmpk.onion/>
You will need to have [Tor](#) installed on your computer to access Tor hidden services.

メールをTorの技術で匿名化

Notice to Officials - Abuse Complaints

This web site is just an informational web page.
None of Tor Mail's mail systems are hosted on this server, or on any server that you can find the IP address.
Siding or shutting down this web site will have no effect on Tor Mail's services.

Tor Mail consists of several servers, a Tor hidden service, and an incoming and outgoing internet facing mail servers.
These internet facing mail servers are relays, they relay mail in and out of the Tor network, the relays are purchased anonymously and not tracable to us.

<http://tormail.org/>

17

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



18

2 次のデジタル・フォレンジック



19

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...

20

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 **過渡期的な対応**
 - 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

- **事後対応の技術的境界**
 - 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…