Responsible disclosureの具体的な事例紹介

情報通信研究機構
サイバーセキュリティ研究所
サイバーセキュリティ研究室

笠間貴弘

横浜国立大学
大学院環境情報研究院/先端科学高等研究院

吉岡克成

※本資料はMWSCISでの吉岡氏の講演資料を基に作成しています

目次

- 研究論文についての概要
- RAID'16での査読コメント
- 実際のResponsible disclosureの流れ

The 19th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2016)

SandPrint: Fingerprinting Malware Sandboxes to Provide Intelligence for Sandbox Evasion

Akira Yokoyama[1], Kou Ishii[1], Rui Tanabe[1], Yinmin Papa[1], Katsunari Yoshioka[1], Tsutomu Matsumoto[1], Takahiro Kasama[2], Daisuke Inoue[2], Michael Brengel[3], Michael Backes[3], and Christian Rossow[1,3(✉)]

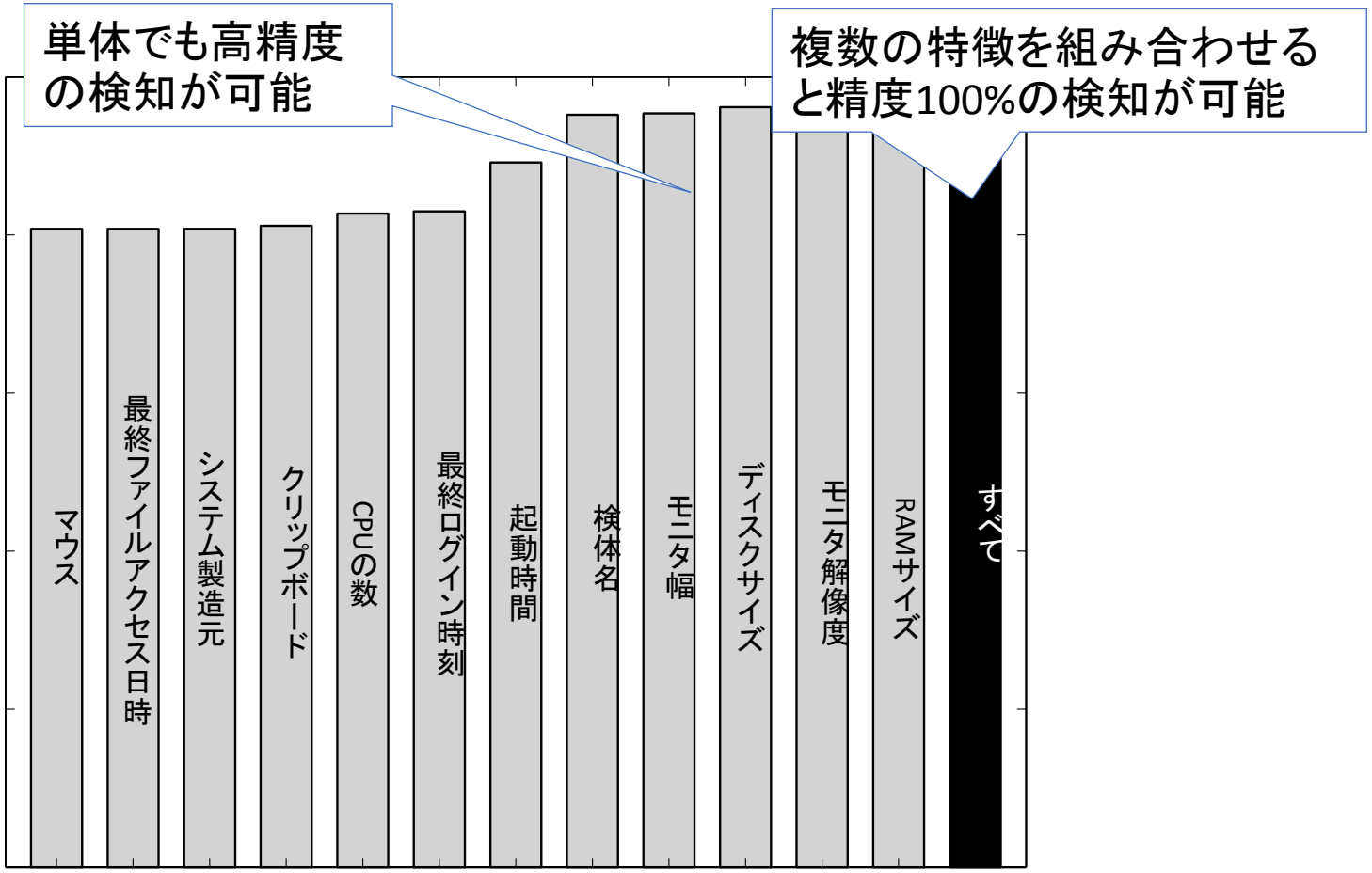
[1] Yokohama National University, Yokohama, Japan
{yokoyama-akira-bs,ishii-kou-yf,tanabe-rui-nv}@ynu.jp,
yinminpapa@gmail.com, yoshioka@ynu.ac.jp,
tsutomu@mlab.jks.ynu.ac.jp
[2] National Institute of Information and Communications Technology, Koganei, Japan
{kasama,dai}@nict.go.jp
[3] Center for IT-Security, Privacy, and Accountability, CISPA, Saarland University, Saarbrücken, Germany
{mbrengel,crossow}@mmci.uni-saarland.de,
backes@cs.uni-saarland.de

Abstract. To cope with the ever-increasing volume of malware samples, automated program analysis techniques are inevitable. Malware sandboxes in particular have become the *de facto* standard to extract a program's behavior. However, the strong need to automate program

論文の概要

- サンドボックス情報収集ツールSandPrintを提案
  - ハードウェア, 履歴, 環境構成, ユーザ操作等の情報を取得
  - ネットワーク経由で収集情報をレポート
- 実在のオンライン解析サービスに投稿し情報収集
  - 世界中の20サービスに定期的に投稿
  - 2666件のレポート収集（33ヶ国の395 IPアドレスから）
- 収集したレポートを学習しサンドボックスを検知
  - オンライン解析サービス＋市販のアプライアンスで検証
  - 全てのサンドボックスを検知可能であることを指摘

高精度でサンドボックス検知が可能



サンドボックス固有な特徴により高精度なサンドボックス検知が可能.

RAID2016の査読コメント

- 結果は条件付き採録
  - Overall merit: 3. Weak accept (Reviewer expertise: 3. Knowledgeable)
  - Overall merit: 2. Weak reject (Reviewer expertise: 3. Knowledgeable)
  - Overall merit: 3. Weak accept (Reviewer expertise: 4. Expert)

(査読コメント抜粋)

It is cool to see that the system also evaluated three security appliances with SandPrint and showed that these systems are even easier to identify compared to public sandboxes. However, this part definitely has ethical considerations as these findings might result in financial implications to these companies.
Definitely, these names should be anonymized in the final version of the paper as promised in section 7.

- Circulating copies of this paper is insufficient to meet the authors obligations to responsible disclosure; the authors are creating new attack techniques and they should notify the malware analysis providers or seek help in doing so if they are unable to do this alone.

RAID2016投稿の裏話

- 論文投稿時は製品名・サービス名は全て実名で投稿(ただし、出版時には製品名を匿名化する予定であることを記載)

- プログラム委員会から「この対応では不十分」との指摘．適切な「Responsible Disclosure」対応をしなければ採録とできない旨のコメントを受ける

- シェパード(論文添削監視者：お世話役)は、イリノイ大学のMichael Bailey准教授であり、**メンロレポートの著者の一人**だった

Responsible Disclosureと論文採録までの流れ

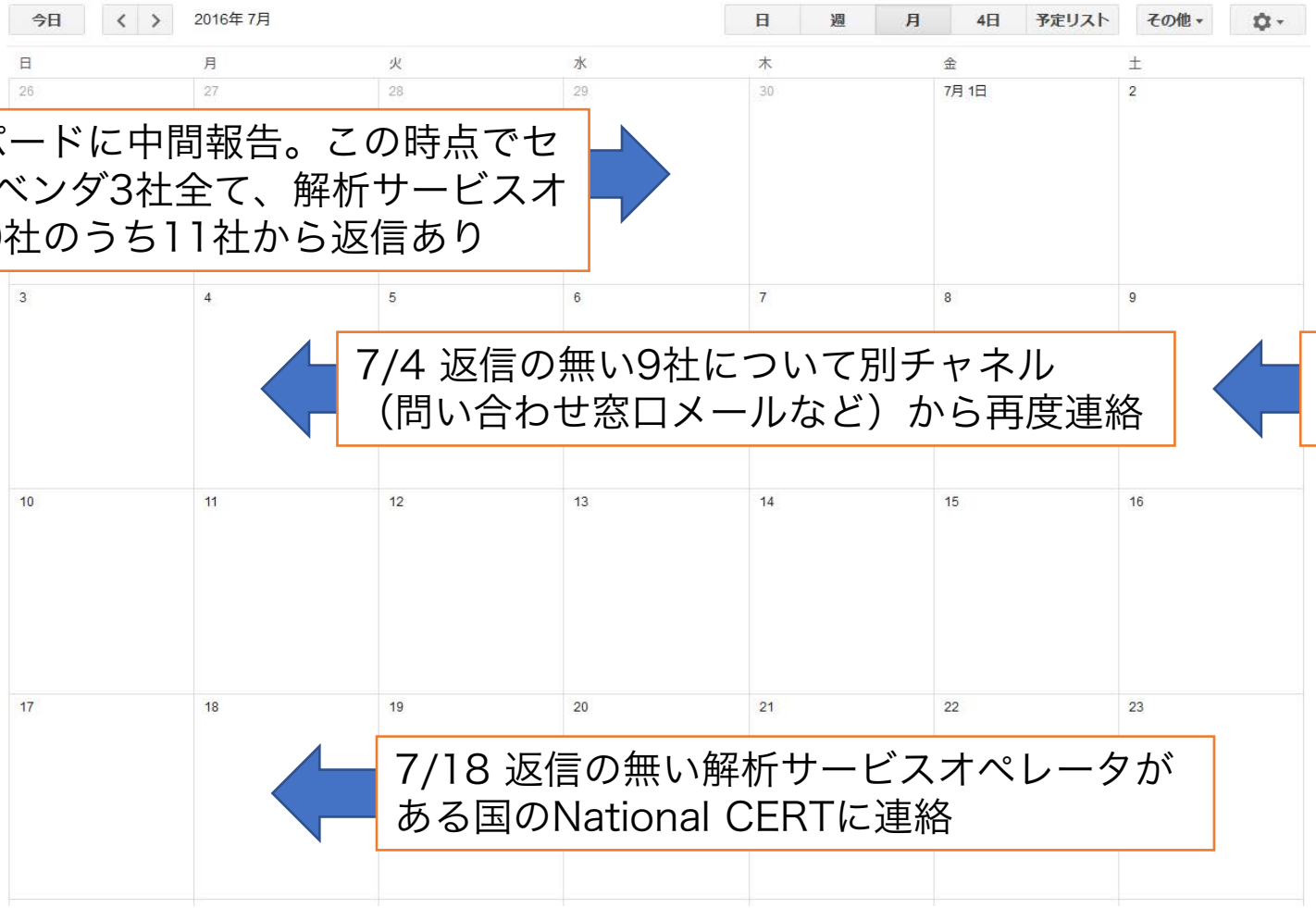
6/4 条件付き採録の連絡が届き
Responsible Disclosureが条件となる

6/10シェパードと著者の各組織が一同にSkype Mtg。
今後のDisclosureの手順について提案し、承認を得る

6/10-20 Disclosureの準備（研究内容と指摘する問題点の説明文、連絡先情報等の確認）

6/21Disclosureの開始（セキュリティベンダ3社＋オンライン解析サービスオペレータ20組織が対象）

Responsible Disclosureと論文採録までの流れ



Disclosureの全体スケジュール

90日間

3つのセキュリティベンダと20のオンライン解析サービスのオペレータに研究内容と脆弱性について通知
(セキュリティ情報提供用メール、または、Webフォームより)

14日間返答がない場合

別のチャネル(各企業の問い合わせ用アドレス等)で連絡

14日間返答がない場合

通知先組織がある国のNational CERTにメール連絡

論文内での記述(約1ページ)

7.1 Ethical Considerations

Our research may seem offensive in the sense that we reveal fingerprints of malware sandboxes that adversaries can use to evade them. Note, however, that the information we presented can be gathered by any other person reproducing our (conceptually simple) fingerprinting method. We thus consider the information shown in this paper as public knowledge. Still, we present data only in aggregated form and refrain from revealing any internals of particular sandboxes.

Using our insights, sandbox operators can
ysis systems. For example, we have shown th
features that are inherent to the snapshot o
be possible to find artifacts that can identif
nificantly harder to build a classifier that wo
more people randomize characteristics. We h
ticularly characteristic of sandboxes, giving
to significantly improve the stealthiness of th

7.2 Responsible Disclosure

Organizations developing sandboxes and/or a
by our research results and we thus consider
responsible disclosure process. To notify these
90 days prior to the publishing date of this pa
and including hints on how to protect against potential adversaries in the future. We used direct contacts whenever possible and available. Alternatively, we resorted to contact details stated on the organization's websites, notably including Web-based contact forms. If we did not receive a response after 2 weeks, we retried to contact the organization, if possible using alternative communication channels (e.g., using generic email addresses like `info@organization.com` or email addresses found in the WHOIS database for the organization's website domain). If we did not hear back from the organization after 4 weeks, we contacted the national CERT(s) that are in the same country as the affected organization in order to notify the party via the CERT as trusted intermediary.

We handed to each organization an executive summary of our research results as well as a full description of our research methodology (i.e., a copy of this paper in the pre-print version). We made sure to highlight the implications of our work with respect to future operations of the sandbox and/or appliance. We also specified our contact details of both research institutions, including physical address, phone number, and the email address of a representative for the research activities. We allowed the organizations to download the latest version of SandPrint and its source code. Such auxiliary data is helpful to build protection mechanisms against sandbox-evasive programs similar to SandPrint. We also remove all organizations' names when referring to individual sandboxes/services.

開示先組織からの反応

- **最終的に１８の組織から研究に対する**
  ポジティブな意見と反応が得られた。

- ネガティブな反応はなかった。

- SandPrintのソースコードを７つの組織に提供した

所感

- Responsible Disclosure等の適切に対応すれば、脆弱性指摘に対するベンダの反応はポジティブなものが多い
  - 友好的な反応を示した組織のうちの１社は以前に匿名化なしに同社製品の脆弱性を詳細暴露した研究者を訴えた実績があった

- Responsible Disclosureには手間と時間が掛かるので、脆弱性研究を発表する場合は、**時間に余裕をもって対応を計画**する必要がある(投稿前にやるべき)

- 必要以上に倫理問題を意識して保守的な研究を行うよりも、世界の動向は**必要な責任を果たして社会への恩恵を高める**研究を評価する傾向にあると考える。(メンロレポートの考え方)