



MWS 2015 ポストイベント MWS Cup 課題1 振り返り

MWS 2015 企画委員

高田 雄太、秋山 満昭、笠間 貴弘、神園 雅紀

2016年1月14日

目次

- 課題内容と意図
- 結果の振り返り
- 回答の紹介
- 今後に向けて

事前準備

悪性 Web サイトへリダイレクトする 改ざんされた一般 Web サイトの発見

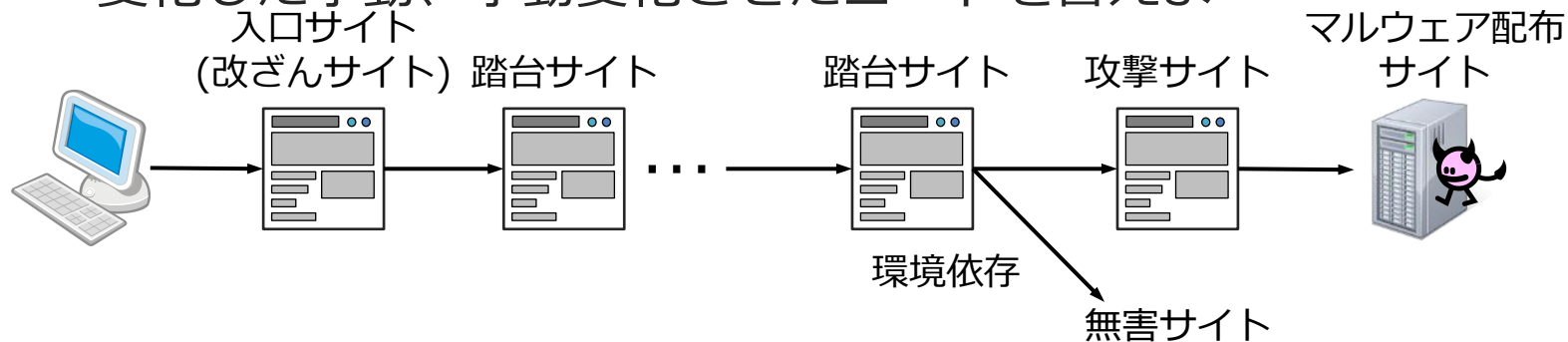
MWS Cup 2015 当日までにドライブバイダウンロード攻撃を仕掛ける悪性 Web サイトへ誘導する**改ざんされた一般 Web サイト**を発見し、根拠情報として発見したWeb サイト情報 (pcap ファイル) を入手せよ。

- 当日までに以下の分析を実施
 - どのような攻撃を仕掛けるか？
 - アクセスする環境によりWeb サイトの挙動* は変化するか？
 - (*) 転送先URLや攻撃コード、マルウェアの変化等を指す

当日課題：課題 1 - 1

発見したWebサイトについて

- 課題 1 - 1 - 1
 - 発見したWebサイトに関連する入口サイト、踏台サイト、攻撃サイト、マルウェア配布サイトのURLを答えよ
- 課題 1 - 1 - 2
 - 悪用された脆弱性のCVE番号を答えよ
- 課題 1 - 1 - 3
 - ブラウザフィンガープリンティングによるWebサイトの挙動変化について、Webサイトの挙動が変化したURL、変化条件と変化した挙動、挙動変化させたコードを答えよ

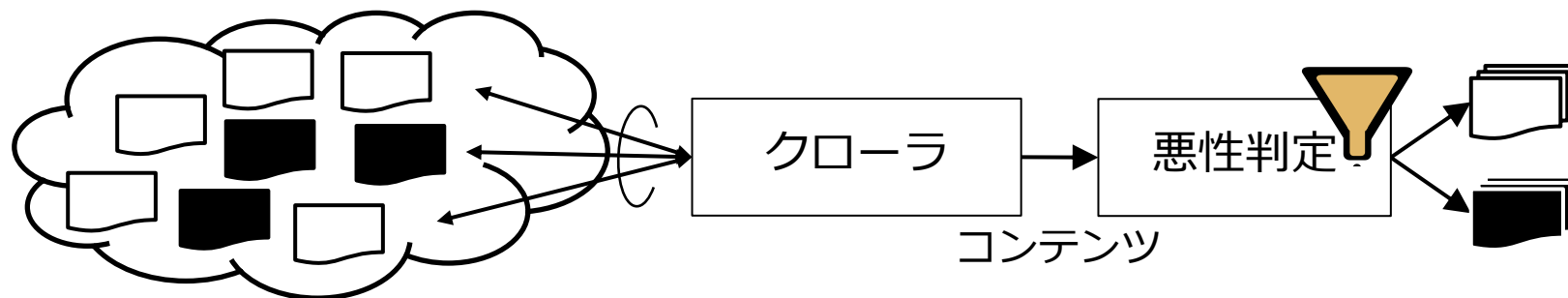




当日課題：課題 1 - 2

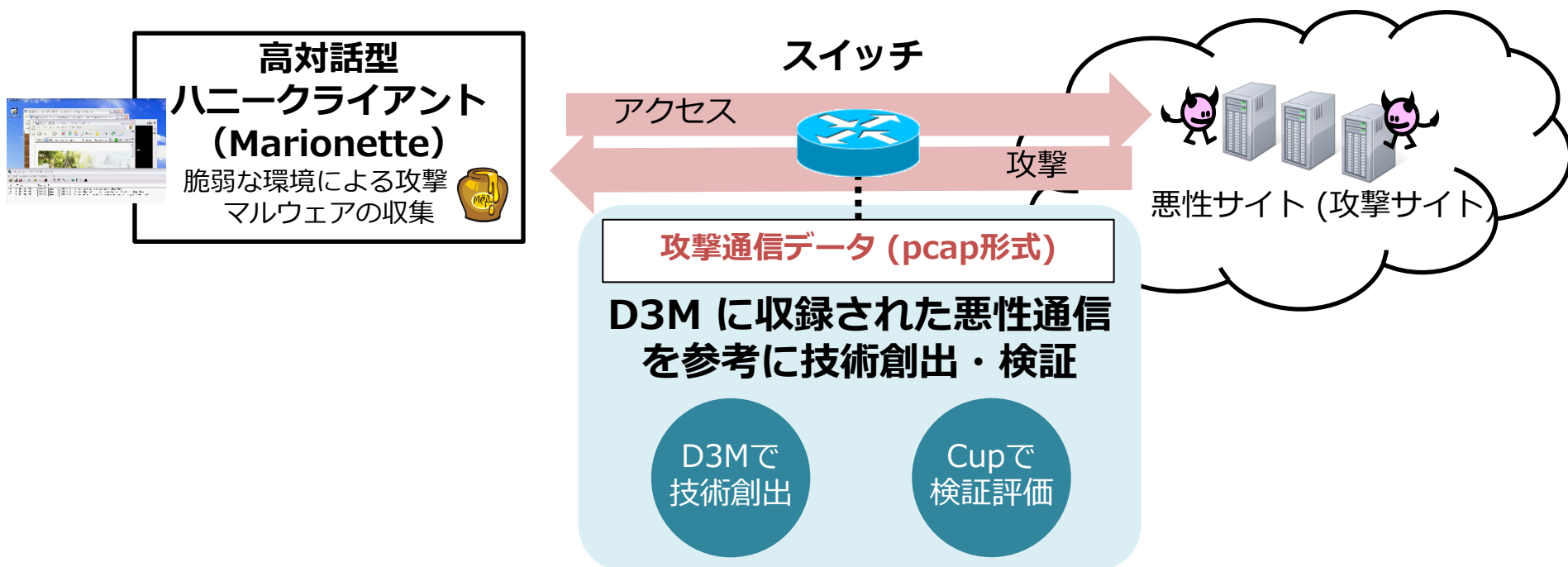
改ざんされた Web サイトの発見と分析について

- 改ざんされた Web サイトを発見したチームは、発見までの過程やアプローチを工夫点とともに 1,000文字以内で述べよ
- or
- 改ざんされた Web サイトを発見できなかったチームは、事前準備に対する試行やアプローチを工夫点とともに 1,000文字以内で述べよ



D3M データセットとの関連性

- ドライブバイダウンロード攻撃に関連する悪性 URL を高対話型ハニークライアント Marionette で巡回し、自動的に発生する一連の Web 通信を収録
 - D3M に収録された悪性情報を悪性 URL へのリダイレクトやマルウェアダウンロード検知に活用





課題の意図 1 / 2

• 大量データの自動解析

- Web サイト巡回、悪性コンテンツ検知・蓄積の**自動化**
 - 今後の研究にも活用可能！MWS データセットとして共有可能！
- “怪しい” Web 空間のみを巡回するには？(巡回の**効率化**)
 - 脆弱なフレームワークや CMS 等の特徴に基づく Google Dork
 - 改ざんキャンペーン情報やスパムメール等の活用
 - など

April 09, 2015

Compromised forums redirect to Fiesta Exploit Kit, distribute malware possibly for click fraud

Google Hacking Database

The Google Hacking Database (GHDB) is a collection of interesting Google searches which find, identify or expose information which could be useful for penetration testers or security auditors such as advertised vulnerabilities, exposed credentials and more.

[Visit the Google Hacking Database](#)

GOOGLE HACKING DATABASE
BY OFFENSIVE SECURITY

WordPress Malware - Active VisitorTracker Campaign

By Daniel Cid on September 18, 2015 . · 12 Comments

MALWARE-TRAFFIC-ANALYSIS.NET



FRIDAY, SEPTEMBER 25, 2015

Compromised WordPress Campaign - Spyware Edition

[Update - October 9, 2015]

Multiple Drupal & Joomla sites affected..

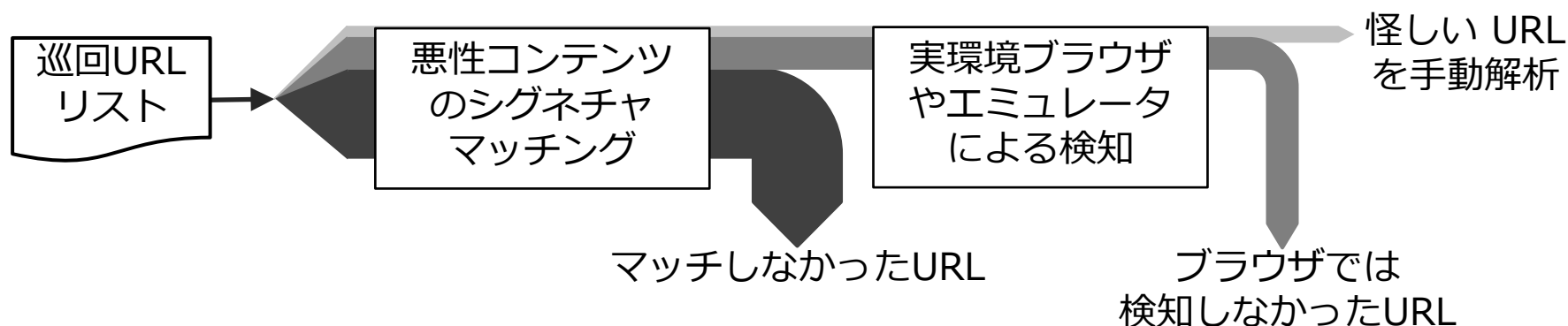
MY BLOG POSTS

- 2015-10-16 -- Angler and 052F gate Nuclear EK fr
- 2015-10-13 -- Angler EK from 188.138.105.137 ser
- 2015-10-12 -- Angler EK from 217.172.170.4 sends
- 2015-10-13 -- Angler EK from 188.138.105.137 ser
- 2015-10-12 -- Angler EK from 217.172.170.4 sends
- 2015-10-08 -- Three examples of Nuclear EK from
- 2015-10-05 -- Nuclear EK from 108.61.189.157 - 2v

課題の意図 2 / 2

・ いかに高速にウェブサイトを巡回・解析するか

- 段階的に解析の粒度を細かくしていき、怪しいウェブサイトのみ手動解析
- たとえば、以下のような構成



結果の振り返り

- 当日の様子
 - 改ざんされたウェブサイトを発見する事前準備が山場であったが、多くのチームが見つげ出し、当日各々の pcap を解析していた
- 採点プロセス
 - 答案を回収した後、課題 1 にご協力いただいた企画委員（笠間さん、秋山さん）で分担し、各チームが収集した pcap をひたすら解析（もうやりたくない）

発見できた URL	チーム数
入口	8
踏台	4
攻撃	2
マルウェア配布	2

URLを発見できたチーム
および惜しかったチーム
の発見方法を紹介

回答の紹介

- 各チームの改ざんウェブサイト発見方法を一部抜粋

悪性ウェブサイト探索の方針

- 脆弱な CMS のみを対象
 - “index of” inurl:wp-content/
- SNS による改ざん情報の活用

巡回方法

- Capture-HPC や Thug による巡回
- Selenium を用いた Firefox による巡回
- HtmlUnit による巡回

巡回URL
リスト

悪性コンテンツ
のシグネチャ
マッチング

実環境ブラウザ
やエミュレータ
による検知

怪しい URL
を手動解析

Exploit Kit の特徴を活用

- 特徴的な文字列を含む URL “052F”
- カラーコード

改ざんらしさの活用

- ブラウザの画面からはみ出るHTMLタグ
- 難読化 JavaScript の検知

なかったURL

検知ログの活用

- Windows Defender ログ
- Fiddler/Capture-HPC ログ
- pcap データ

今後に向けて

- **ツールの共有**

- シードURL選定スクリプトや巡回スクリプト等
- 似たようなことは再度やる必要はない

- **短命な悪性 URL と観測環境の網羅**

- 攻撃を検知した際に関連する URL を共有する仕組み／コミュニティが必要
- さまざまな環境（IP アドレス、OS、ブラウザ、プラグイン、言語設定等）でウェブ空間を観測する必要有り