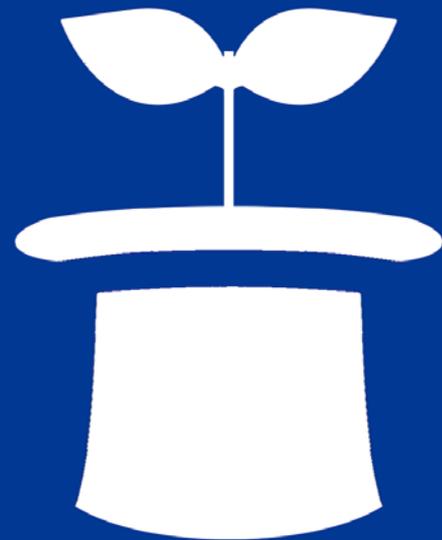


MWS



MWS Cup 2015

課題 1 : Drive-by Download 攻撃解析

MWS 2015 企画委員

高田 雄太、秋山満昭、笠間 貴弘、神園 雅紀

2015年10月21日



担当および課題作成協力者

- 課題作成協力者

- 秋山 満昭 NTT セキュアプラットフォーム研究所
- 笠間 貴弘 国立研究開発法人情報通信研究機構
- 神薊 雅紀 国立研究開発法人情報通信研究機構

- 担当

- 高田 雄太 NTT セキュアプラットフォーム研究所

※<http://www.iwsec.org/mws/2015/committee.html>



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。
なお、発見した Web サイトについて、以下の内容を分析すること。

- 改ざんされた Web サイトは、どのような攻撃を仕掛ける悪性 Web サイトへリダイレクトしたか？
- ブラウザフィンガープリンティング等により取得した情報に応じて、クライアント側でWeb サイトの挙動* は変化したか？
 - (*) 転送先URLや攻撃コード、マルウェアの変化等を指す
- Referer 等のパラメータやアクセス回数に応じて、サーバ側でWeb サイトの挙動が変化したことを推測できるか？

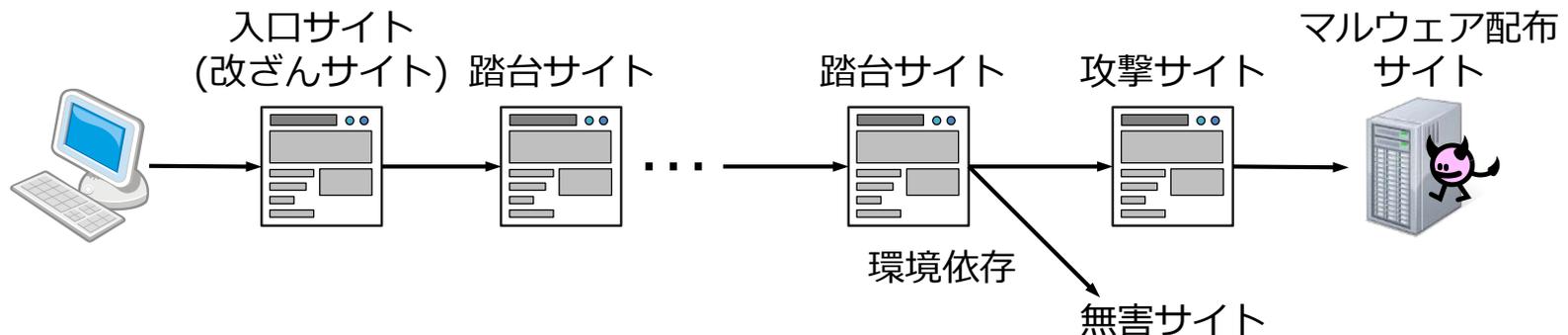
ボーナス点として、発見した Web サイトが MWS Cup 2015 当日の Alexa に掲載されている場合は、順位および発見日時等に応じて最大 3 点まで加点。



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

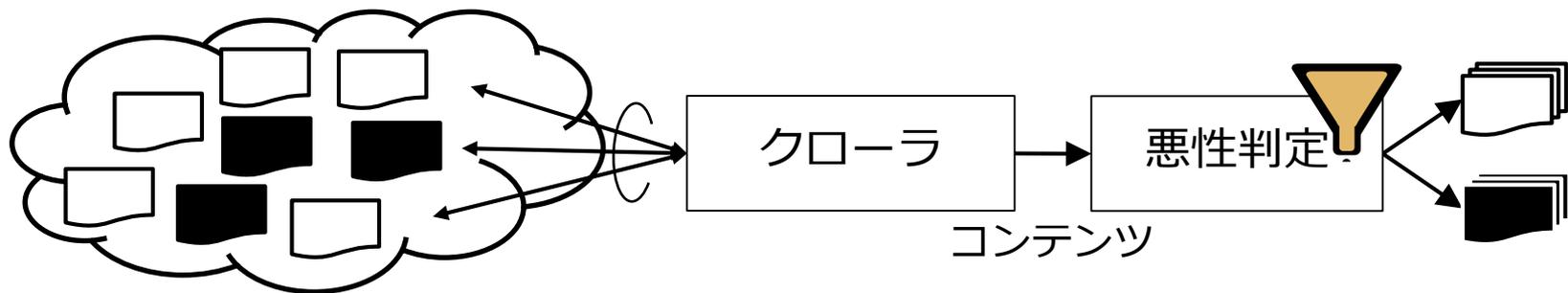




当日課題：課題 1 – 2

改ざんされた Web サイトの発見と分析について

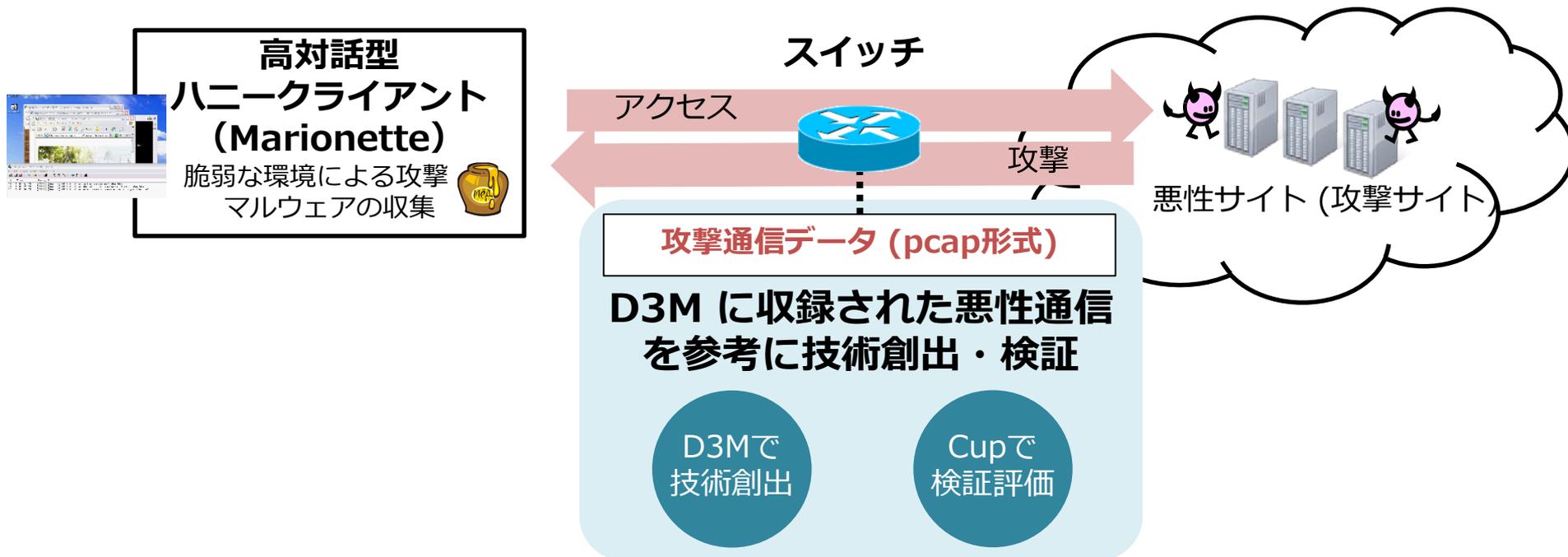
- 改ざんされた Web サイトを発見したチームは、発見までの過程やアプローチを工夫点とともに 1,000文字以内で述べよ
- or
- 改ざんされた Web サイトを発見できなかったチームは、事前準備に対する試行やアプローチを工夫点とともに 1,000文字以内で述べよ





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..

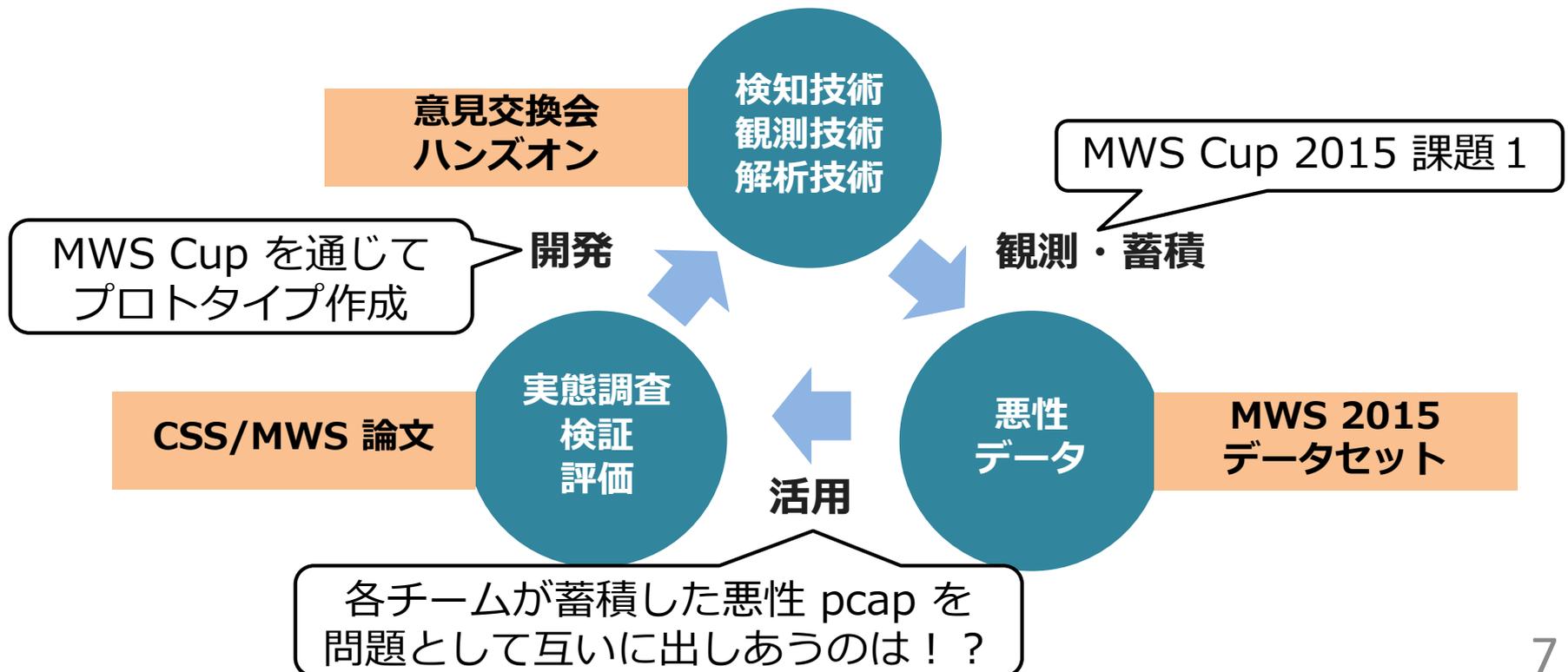
MY BLOG POSTS

- 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 send
- 2015-10-13 -- Angler EK from 188.138.105.137 ser
- 2015-10-12 -- Angler EK from 217.172.170.4 send
- 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

- 問題を各チームで用意してもらおう新スタイル
 - **用意された悪性 Web サイトの解析**や**用意された悪性 pcap の解析**は、意見交換会やハンズオンでカバー
 - MWS Cup を通じて**研究の着想**を得てもらい、**新技術の創出**や**実用的な技術への深化**を期待





参考情報

- 八木, 秋山, 村山
コンピュータネットワークセキュリティ
コロナ社
- 8章で「悪性サイトの発見」
について解説

