MWS Cup 2013
事前課題 4「予兆検知から駆除・無効化のシナリオ設計」解答例

1. 出題の意図

MWS[1]で研究用データセット[2]として提供している PRACTICE Dataset 2013 には Zero Access[3][4][5]に関するデータセットが含まれている. データセットの分析および各種文献から，具体的なマルウェア対策に向けたアイデアを生み出しデータセットの提供元である PRACTICE にフィードバックを行う. なお，出題にあたっては具体的なマルウェアを指定することで，解答内容の具体化・詳細化を期待したものである.

2. 出題内容

PRACTICE Dataset 2013 に収録されている長期観測通信データや、各種公開レポート、既存のマルウェア対策に関わる文献を参考に、日本においても感染ノードが多く観測されているマルウェア Zero Access の対策について、以下の設問に各 800 字以内で答えなさい。なお、採点は手法としての新規性よりも、実現性・有効性を重視し、解答には対策にあたっての前提条件も含めること。

[設問 1] ドライブ・バイ・ダウンロードによる感染、攻撃（感染後にダウンロードした検体による挙動含む）や攻撃基盤（P2P 型ボットネット）の変化を早期に検知するためには、どのような観測・分析を行うのが良いか述べよ。(5 点)

[設問 2] パッチ適用やアンチウイルスソフトの導入といった感染予防策がわかっていたとしても、感染者（感染端末）が出てしまう現状がある。また、駆除ソフトを配布して駆除するという方法が有効に機能するためには、感染者（感染端末）への何らかの通知が必要となる。これらを踏まえ、効果的に駆除・無効化する方法を述べよ。

3. 解答例

MWS Cup 2013 参加チームから提出された事前課題レポートより，解答内容を抜粋・要約する．文末の（）内は参加チーム名を表す.

3.1. 設問 1

- ダウンロードする DLL の更新によるボットコマンドの追加や変更の追跡，コマンド送受信時の XOR のキーの変更を検知．(Alkaneters)
- 開環境の動的解析による通信開始時の固定的なバイト列の変更を検知．(人海戦術チーム)
- NAT 無しのインターネット接続環境で Super node になって update や通信パターンの変化を検知．一部ハードコーディングされている接続先 IP アドレスや，ハードコーディングされている利用ポート番号の変更を検知．(WeightAnkle teamBy Res9)
- 利用ポート別のトラフィックの周期性の変化や利用ポートの変化を検知．(Team Enu)
- API フックによるコマンドの特定とパケット分析によりボットコマンドの変更を検知．(セキュリティ謳歌)
- 感染端末からのパケットに応答を返すアドレス数の変化を検知．(GOTO Love and 初代森研)
- 感染後に接続するダウンロードサイトを一定間隔で監視し、検体の入れ替えが行われることを検知．感染端末にダミーデータを入れておき，どのように不正利用されるかを監視．DGA(Domain Generation Algorithm)から判明したドメイン名を購入し，そこにアクセスしてくる端末を観測することで変化を検知．(KIT-C-UT)
- 複数の開環境動的解析機間のトラフィック変化を検知．(Olab 2013)

3.2. 設問 2

- 組織内 PC とスーパーノードの接続をポートベースでフィルタイング．newL コマンドによって Zero Access が保持するスーパーノードのアドレスリストを無害なものへと書き換え．P2P ネットワークで配信される更新ファイルとして「感染による改変箇所の修復スクリプト」を放流．(Olab 2013)
- 改ざんされていたコンテンツ・改ざんされていた期間・アクセスしたことによって起こりえる影響・対処法等を記載した Web コンテンツを作成し，注意喚起．(頑張ります)
- 広告クリックなどの規則性や時間帯毎の周期性，クリックされる広告の

種類の不規則性などから，広告業者が潜在的な感染ユーザを推測．Yahoo Japan や Google といったポータルサイトへ，改ざんされた Web サイトの情報を報告し，検索結果などで警告．(TDUISL in 親方)

- 企業や学内の対策として，Windows Server によるレジストリのグループ管理機能を用い感染している端末のレジストリ情報を更新．(SecCap のゆかいな仲間たち)
- テレビ放送によるパッチ適用やアンチウイルスソフトの導入を呼びかける広告やニュースを放送．ホームルータにおいてマルウェアを検知する仕組みを組み込み．Windows Update において Zero Access を駆除するソフトウェアを配布．(人海戦術チーム)

4. PRACTICE Dataset 2013

PRACTICE Dataset 2013 は総務省「国際連携によるサイバー攻撃予知・即応に関する実証実験」（略称：PRACTICE）の挙動観察システムで，5 検体のマルウェアを長期観測（最大 1 週間程度）した際の通信トラヒック（マルウェア感染後の通信挙動）を示すデータセットである．本データセットは，マルウェア感染後の通信挙動や通信先の分析，検知手法の評価，解析環境の課題提起に利用することを想定している．データセットは検体そのものを含まず，検体情報と通信トラフィックデータで構成され，以下で概要を述べる．

4.1. 検体情報

検体情報には検体のハッシュ値（sha1），取得した通信トラフィックデータ（libpcap 形式）のファイル名，解析環境の IP アドレス，4 種類のアンチウイルスソフトでの検知結果（各検体収集時点で最新のパターンファイルを利用），解析開始時刻・終了時刻，ファイルサイズを含む(表 1)．

4.2. 通信トラフィックデータ

通信トラフィックデータを取得している各検体の動的解析環境は Botnet Watcher[6]であり，データには，インターネットへの疎通確認や時刻同期など管理用通信も一部含んでいる．また IP アドレス，デフォルト GW，DNS サーバは DHCP で割り当てている．TCP/UDP ともにランダムあるいは一定の high port を利用した P2P 通信を行っている検体や，繰り返し IRC 接続を試みる検体，何らかのファイルをダウンロードしている検体など，特徴的な通信挙動が確認できる．しかしながら，接続先の名

前解決ができないものもあり，検体の収集直後からの解析が望ましい.

表 1　検体情報の例

項目	例
ハッシュ値(sha1)	5b9f7***
pcap ファイル名	practice_1.pcap
IP アドレス	10.220.0.36
検知結果	Kaspersky: 未検知 McAfee: PWS-Zbot.gen.alu Symantec: 未検知 TrendMicro: 未検知
解析時刻	2013-05-18 02:35:06～2013-05-25 11:59:53
ファイルサイズ	10MB

5. 総評

Web 巡回型ハニーポットによる感染の検知・検体収集，収集検体の開環境動的解析，感染ユーザへの注意喚起，駆除ツールへの誘導など，PRACTICE の取り組みに準じる内容の解答も多数あった．一方で，新たなアイデアを実現していくためには，従来の枠組みを超えた各組織との連携を深める必要性があることもわかる．具体的には，各所で Zero Access 感染端末の開環境動的解析をスーパーノード含めて行ってその解析結果を共有したり，大学等ネットワークにおけるトラフィック観測による検知方法を実証することで有効性を定量評価したりすることが挙げられる.

また，感染源となる改ざんされた Web サイトの管理者に通知をして改ざんを修正する以外にも，改ざんを受けた内容やその間のアクセス者(潜在的な感染者)の情報を活用できれば，より効果的な注意喚起につながるかもしれない．もちろん，このような対策を実施するにあたっては，各サービスにおけるユーザ同意が必要になるため，可能な範囲から始めざるを得ない点も注意したい.

参考文献

[1] マルウェア対策研究人材育成ワークショップ(MWS: anti-Malware engineering WorkShop), http://www.iwsec.org/mws/2013/

[2] 神薗，他：マルウェア対策のための研究用データセット ～ MWS Datasets 2013 ～, http://www.iwsec.org/mws/2013/manuscript/1A1-1.pdf, MWS2013

[3] SophosLabs UK, “ZeroAccess”, http://www.sophos.com/ja-jp/why-sophos/our-people/technical-papers/zeroaccess.aspx

[4] IIJ, “Internet Infrastructure Review （IIR） Vol.20”, http://www.iij.ad.jp/company/development/report/iir/020.html

[5] Rossow, C. et al: SoK: P2PWNED - Modeling and Evaluating the Resilience of Peer-to-Peer Botnets, IEEE S&P2013

[6] Kazufumi Aoki, et al: Controlling Malware HTTP Communications in Dynamic Analysis System using Search Engine, IEEE CSS2011