ユーザ環境観測によるRIG Exploit Kitの長期観測と時間変化に対して頑強な攻撃検知

嶌田 一郎[†1]　太田 敏史[†1]　山田 明[†2]

概要：現在，Webサイトを閲覧することによってマルウェアに感染させるDrive-by Download(DBD)攻撃が深刻な問題となっている．この攻撃は，Exploit Kit(EK)と呼ばれる攻撃基盤の上で行われることが多く，なかでもRIG EKが近年もっとも大きな被害を与えた．RIG EKは，攻撃の特徴であるIndicators of Compromise (IOC)によって検知されるが，踏み台サイトの取り締まりや攻撃検知の回避のためにIOCが変化してしまうため，攻撃を継続的に観測することが困難であるという課題があった．本研究では，あるセキュリティツールの7ヶ月間の長期ログを分析することによって，RIG EKの長期活動を明らかにする．このなかで，変化するIOCに対して，自動的に導出する検知方式を提案する．提案方式を評価した結果，RIG EKドメイン名を平均98%の再現率(recall)，50%の適合率(precision)で検知できることを確認した．また，期間中のIOCの変化に追従して，新しいIOCを導出できることが明らかになった．

キーワード：Web媒介型攻撃，Drive-by Download，RIG Exploit Kit

Long-Term Observation of RIG Exploit Kit by User Environment Observation and Robust Attack Detection Against Time Change

Ichiro Shimada[†1]　Toshifumi Oota[†1]　Akira Yamada[†2]

Abstract: Recently, drive-by download (DBD) attacks that infect computers with malware when users browse infected websites have been a serious problem. These attacks are often done on an attack base called an exploit kit (EK); among them, RIG EK has been causing the most serious damage. Since DBD attacks occur in a user's web browser, it is difficult to grasp the whole image of the attack. Also, although they are detected using indicators of compromise (IOC), which is a characteristic of attack, IOC changes due to crackdowns on a stepping stone site and avoiding attack detection are a problem. In this research, we analyzed the long-term logs of a certain security tool for 7 months to clarify the long-term activities of RIG EK. Then, by automatically deriving a new IOC, we proposed a robust detection method against changes in the IOC of RIG EK. By evaluating the proposed method, we found that RIG EK domain name could be detected at a recall ratio of 98%(average) and a precision ratio of 50%(average). We also found that a new IOC can be derived after changing the IOC during the period.

Keywords: Web-based cyber attack, Drive-by Download, RIG Exploit Kit

1. はじめに

現在，Webサイトを閲覧することによってマルウェアに感染させるDrive by-Download(DBD)攻撃が深刻な問題となっている．日本年金機構への初段攻撃も，メール記載のURL リンクのクリックによる Web アクセスから発生したという報告がある[1]．DBD攻撃は，更に巧妙化，高度化してきており，特定のユーザのWebアクセス特性を攻撃に利用する水飲み場攻撃が出現するなど，脅威が拡大しており，Webページ改ざんの実態，及び被害規模を大局的に把握する方法の確立が求められている．

DBD攻撃は，Exploit Kit(EK)と呼ばれる攻撃基盤の上で行われることが多く，なかでもRIG EKが近年もっとも大きな被害を与えた．DBD攻撃は，ユーザのWebブラウザにおいて発生するため，攻撃の全体像を把握することが難しい．また，攻撃の特徴である Indicators of Compromise (IOC) を用いて観測できるが，踏み台サイトの取り締まりや攻撃検知の回避のためにIOCが変化してしまうという課題がある．本論文において，RIG EKのIOCの変化に対して頑強な検知方式の提案と評価を行った．

以下，2章では，関連研究について述べ，3章では，攻撃の観測について述べる．4章では，RIG EKの長期観測結果について述べる．そして，5 章では，分析の前処理について述べ,6 章では,時間変化に頑強な攻撃検知について述べる.7 章で実験と評価について述べ,8 章でまとめを述べる．

2. 関連研究

Webアクセスログから効率的に悪性サイトを抽出する手法の研究として[1]がある．[1]では，高速に検査対象URLを絞り込む前段処理と，低速だが精度の高い詳細分析を行う

†1 株式会社構造計画研究所
KOZO KEIKAKU ENGINEERING Inc.
†2 株式会社KDDI総合研究所
KDDI Research, Inc.

© 2018 Information Processing Society of Japan

後段処理により，効率良く膨大な Web アクセスログから悪性サイトを抽出する手法の提案，及び評価実験を行っている．

RIG EK のキャンペーンの特徴の調査を行った研究として[2]がある．[2]では，複数の攻撃キャンペーンを探索するプログラムを実装し，決定木により RIG EK の攻撃キャンペーン毎の特徴を分析している．また，[3]では，RIG EK を長期間追跡し解析妨害手法を明らかにするとともに，追跡過程で得られた情報により RIG EK で利用されているドメインをテイクダウンすることに協力し，一時的に活動を停止させることに成功している．しかし，[4]の報告によると，RIG EK は依然として活発に活動している．ドメインのテイクダウンについては，3 章で述べる．

EK により構築された悪性 Web サイトの URL に現れる特徴に関する研究として[5]がある．[5]では，様々な EK による URL の特徴をシグネチャとして利用することで，DBD 攻撃の全体把握を容易にするための研究を行っている．また，[6]では，サイト関連情報を特徴量として利用し，Random Forest を用いて RIG EK の識別が可能であることを示している．また，分類により得られた URL の構造の特徴，分類に有効な特徴について研究を行っている．この他，既知悪性 URL の特徴を利用して，Bayesian Sets によって悪性 URL と近い特徴を持つ URL を特定する手法[7]，WHOIS の応答を TF-IDF による特徴を用いて Landing Domain と Distribution Domain の分類を行う手法[8]，などがある．

悪性 Web サイトの生存期間に関する研究として [9]がある．[9]では，おとりとして動作する Web サイトを用いることで，攻撃者による Web 改ざんを誘い込み，リダイレクト先の悪性 Web サイトの活動を受動的に観測し，観測された期間のみをブラックリストへ登録している．悪性サイトは短期間で変化し，約 80%はわずか 1 日だけ利用され，残りの約 20%は数 100 日以上利用されるものも存在したと分析されている．また著者らは,[10]においてユーザ環境から収集した大規模な Web アクセスログの観測結果から RIG EK のドメイン生存期間が短時間であると推測した．

悪性サイトに関する大規模な実態調査を行った研究として[11-13]がある．[11]では，ひと月に 1800 万 URL をクローリングし Drive-by Download やスパイウェアの観測を行っている．[12]では，数十億 URL を分析し 45 万 URL の Drive-by Download 攻撃を検出している．[13]では，10 ヶ月間で 6000 万件以上の URL を観測し，300 万件以上の悪性 URL を検出している．また，Drive-by Download に係る悪性サイトの広域な観測網のためのフレームワークとして FCDBD(Framework for Countering Drive-by Download)[14-15]の研究がある．FCDBD は，発見，検出及び防御を目的としている．

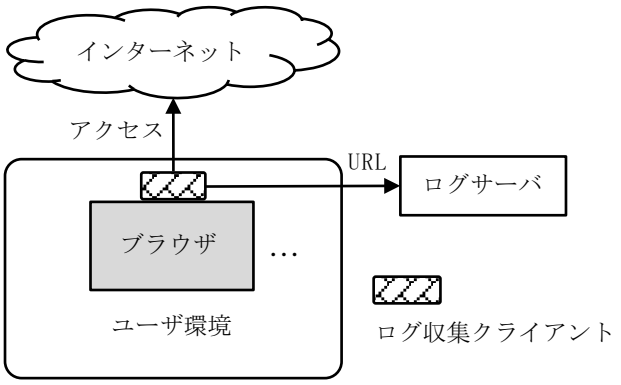

図 1 観測環境の概要

Figure 1 Overview of Observation environment.

本研究では，RIG EK に焦点をあて，大規模な Web アクセスログを用いた観測により，RIG EK の長期活動を明らかにする．また，機械学習を用いて RIG EK の IOC の変化に対して頑強な検知方式を提案する．さらに，この検知方式に基づいて，新しい IOC を自動的に導出する方式を提案し，検知手法の評価を行う．

3. 攻撃の観測

本章では，まず RIG Exploit Kit の特徴について述べ，次に IOC による検知方法，観測で使用した環境について述べる．

3.1 RIG Exploit Kit

RIG Exploit Kit を使用した典型的な攻撃手順は以下の通りである[18].

(1) 閲覧者の感染サイト訪問

感染サイトには，悪意のあるドメインから JavaScript を読み込むインジェクションコードが含まれる．

(2) Exploit Kit ゲートによる攻撃対象判断

ゲートの機能は，閲覧者がキャンペーンの対象範囲か，つまり閲覧者のプラットフォームが攻撃対象か，または閲覧者が攻撃対象の地域からアクセスしているか判断する．

(3) ランディングページ

ランディングページに実際の不正コードが読み込まれる．キャンペーンに応じて，ランディングページへのリンク，追加のペイロード，パラメータや変数としてエンコードされた暗号化キーを含めることができる．

(4) Exploit 実行

閲覧者に不正コードを読み込ませることに成功すると，長いパラメータを持つ cmd.exe が呼び出され，難読化された JavaScript が書き込まれ，JavaScript はランディングページによって生成されたパラメータで実行される．

(5) ペイロード配信

ペイロードは，特定のキャンペーンに依存しており，Cerber や Locky などのランサムウェアは，現在の RIG キャンペーンの一般的なペイロードである．

© 2018 Information Processing Society of Japan

本研究の対象 IOC は，攻撃手順(1)の RIG EK サイトアクセス時の URL パラメータ部分に現れる．IOC による検知方法については，6 章で述べる．

3.2 観測環境

本研究では，大局的に実態を把握するために，多数のエンドユーザから収集した大規模な Web アクセスログを利用し調査を行った．本研究で用いた観測環境の概要を図 1 に示す．

ログ収集クライアントは，あるセキュリティベンダが提供するソフトウェアである．ログ収集クライアントは，ブラウザに組み込むプラグイン・ソフトウェアであり，ユーザが個別にダウンロードして利用することができる．ログ収集クライアントはユーザ数が非常に多く，大規模な Web アクセスログデータの収集が可能である．ログ収集クライアントが収集するログデータ（以下，ログデータ）は，ユーザが Web アクセスした時のログデータであり，データ内容は，アクセス時刻，匿名化されたユニークユーザ ID，アクセス先 URL，アクセス先ドメイン名で構成される．

ユーザがブラウザからインターネットへアクセスした時の Web アクセスログは，ログサーバ経由で保存される．このため，ユーザが改ざんページ上に埋め込まれた RIG EK の特徴を持つ URL(以下，RIG EK URL)にアクセスすると，そのアクセス履歴もログサーバ経由で保存される．

本研究では，保存された研究用ログデータを利用して RIG EK の Web アクセス状況の分析を行った．観測期間は，2017 年 2 月 1 日から 2017 年 8 月 29 日までの 7 ヶ月間であり，1 日あたり 24 時間分の連続したログデータを対象として観測を行った．図 2 に，観測期間の Web アクセスログ数の推移を示す．

3.3 ユーザ環境での観測の特徴

悪性サイトの観測手法には，Web サーバハニーポットを用いて DBD 攻撃を受動的に観測する受動的観測，Web クライアントハニーポットを用いて能動的に悪性サイトをクローリングして観測する能動的観測があり，悪性サイトの観測に活用されている．本研究では，3.2 節で述べたユーザ環境での観測手法を用いた．ユーザ環境での観測は，下記の特徴を持つ．

(1) 実際にユーザが Web アクセスした際のログデータであり，現実のアクセス状況が観測できる．

(2) 大規模なユーザ環境でのログデータを収集することで，DBD 攻撃の大局的な実態把握の検討ができる．

本研究では，これらの特徴を持つユーザ環境での観測結果を活かし，RIG EK の IOC の変化に対して頑強な検知方式の検討を行った．

4. RIG Exploit Kit の長期観測

4.1 IOC による検知方法

本研究では，RIG EK URL 上の部分文字列を IOC として検知に使用した．使用した IOC の内容を，表 1 に示す．表 1 の IOC については，パターン 1–3 は[16]を，パターン 4–35 は[17]を参考にしている．

表 1　RIG EK の IOC
Table 1　IOC of RIG EK.

IOC パターン	IOC 内容
1	QMvXcJ
2	WrwE0q
3	fPrfJxzFGMSUb-nJDa9
4	Qc_Wfa
5	Qc_WYa
6	Qc_WZa
7	Qc_Wea
8	Qd_Wda
9	Qd_Wea
10	Qd_Wfa
11	QcvWda
12	QcvWea
13	QcvWfa
14	QcvWYa
15	QcvWZa
16	QdfWda
17	QdfWea
18	QdfWfa
19	QdfWYa
20	QdfWza
21	QdPWda
22	QdPWea
23	QdPWfa
24	QdPWYa
25	QdPWZa
26	QMrDYb
27	QMrLYb
28	QMrPYb
29	QMrTYb
30	QMrXYb
31	QMvWdb
32	QMvWeb
33	QMvWfb
34	QMvWYb
35	QMvWZb

4.2 観測結果

表 1 の IOC パターンに基づき，2017 年 2 月 1 日から 2017 年 8 月 29 日迄の 7 ヶ月間に渡る Web アクセスログの観測結果を，図 3 に示す．IOC パターンは，2017 年 6 月 13

© 2018 Information Processing Society of Japan

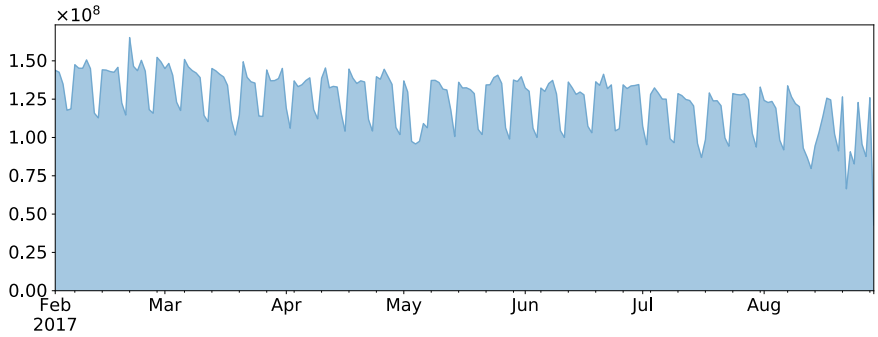

図 2　観測期間の Web アクセスログ数の推移

Figure 2　Transitions in the number of Web access logs during the observation period.

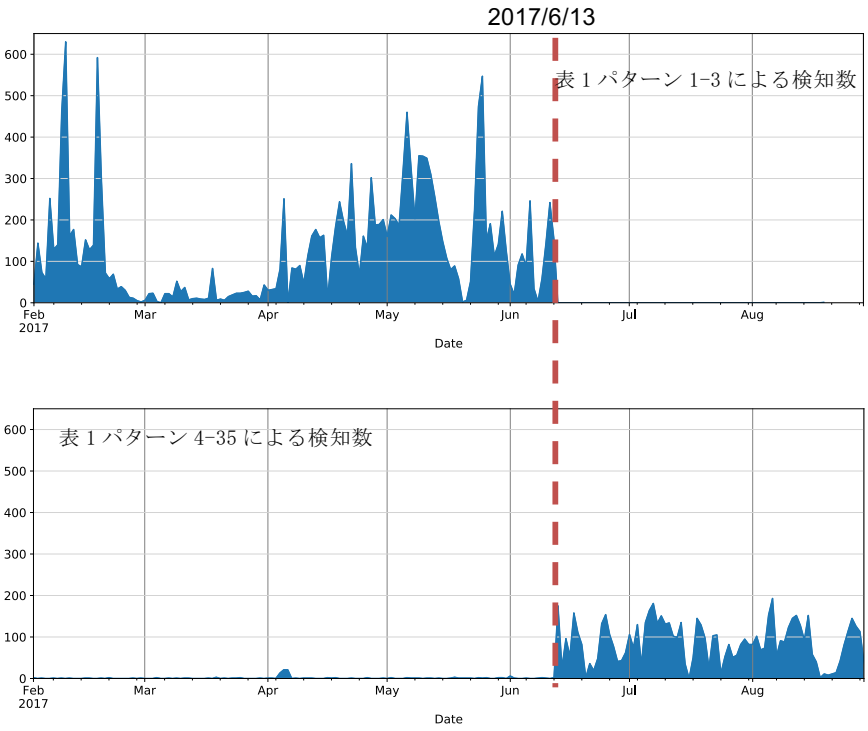

図 3　RIG EK の検知結果

Figure 3　Result of RIG EK detection.

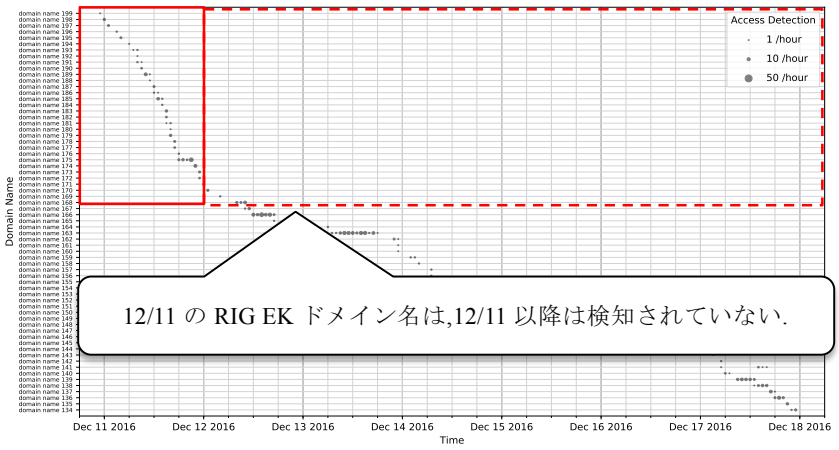

図 4　RIG EK ドメイン名へのアクセス数(2016 年 12 月 11 日～17 日)とホワイトリスト利用の概念図

Figure 4　The number of accesses to the RIG EK domain name (11th December to 17th December 2016) and conceptual diagram of whitelist utilization.

© 2018 Information Processing Society of Japan

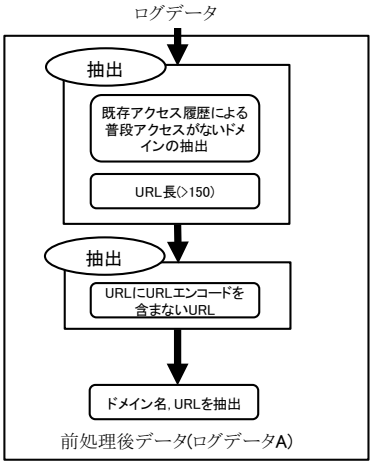

図 5　分析の前処理フロー

Figure 5　Preprocessing flow for analysis.

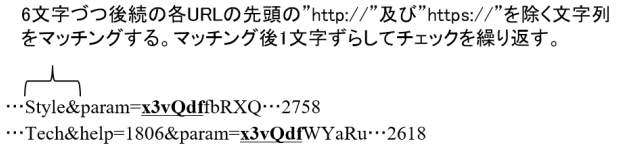

図 6　部分文字列の抽出方法

Figure 6　Method of extracting substrings.

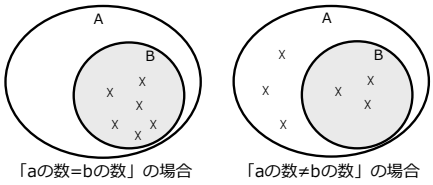

図 7 部分文字列選出の概念図

Figure 7　Conceptual diagram of substring selection.

日を境に変化しており，Domain Shadowing のテイクダウン[18]によるものと考えられる．Domain Shadowing のテイクダウンについては，次節で述べる．

4.3 Domain Shadowing のテイクダウン

Domain Shadowing とは，攻撃者がドメイン登録者のアカウントを乗っ取って，正常なサイトのサブドメインに攻撃サイトを構築する手段である[18]. 2011 年頃から観測され，Angler EK でも利用された．

[18]によると，RSA Research は，RIG EK のランディングページのサブドメインを，Whois 登録の詳細や，ドメインや URL に関連する情報を自動的に収集・可視化するツール Maltego[19] を用いて調査した結果，レジストラ GoDaddy[20]を主要なレジストラとして特定した．RSA Research は，GoDaddy と協力し，Domain Shadowing のテイクダウンを実施している．前節で述べた，IOC のパターン変化は，テイクダウンの影響と推測している．

5. 分析の前処理

RIG EK を検知するためには，3 章の観測結果で示した通り，約 1 億数千万 URL/日と膨大な Web アクセスログから悪性な Web アクセスを抽出する必要がある．そこで，効率的に RIG EK の分析を行うための前処理として，次の方法により分析対象ログデータ数の削減を行った．

(1) ホワイトリストの利用

(2) RIG EK URL の特徴の利用

以下，各手法について詳述する．

5.1 ホワイトリストの利用

RIG EK の活動期間が数時間と短時間である特徴を利用し，全ユーザの過去の Web アクセスログをホワイトリストとして利用する手法により分析対象ログデータ数の削減を行った．具体的には，ある一定期間(例えば，1 日間)に検知された RIG EK のドメイン名は，その期間の後(例えば翌日)は検知されていない．このため，既知のドメイン名は活動していないものと見なし，ドメイン名のホワイトリストに登録した．ホワイトリストを活用し，普段は Web アクセスがないドメインへのログデータだけを効率よく抽出した．RIG EK ドメイン名アクセス検知数(2016 年 12 月 11 日～17 日)とホワイトリスト活用の概念図を図 4 に示す．

5.2 RIG EK URL の特徴の利用

ホワイトリストによる絞り込んだ結果を，更に RIG EK URL の特徴を利用することで，分析対象ログデータ数の削減を行った．特徴として利用したのは，次の通りである．

(1) URL 長

(2) URL エンコードの有無

RIG EK の URL 長(文字数)に着目した既存研究としては，[6]がある．[6]によると，RIG EK の URL 長には，ある一定の URL 長以上であるという特徴がある．本研究においても URL 長に着目した．2017 年 6 月 8 日～2017 年 6 月 17 日まで期間で検知した RIG EK の URL 長から，150 文字を超える URL 長を持つログデータを抽出した．

更に，RIG EK URL の特徴として，URL エンコードを持たない特徴が見られた．このため，URL エンコードを持つ URL は対象外とした．図 5 に手法全体の概念図を示す．分析対象として抽出したログデータ(以下，ログデータ A)は，ドメイン名と URL で構成される．

6. 時間変化に頑強な攻撃検知

6.1 IOC 自動導出アルゴリズム

5 章の分析の前処理で抽出したログデータ A から，RIG EK の IOC を導出する方法について述べる.以下の手順で導出した．

(1) RIG EK ドメイン名，URL の抽出

IOC を用いて RIG EK ドメイン名と URL を抽出する(以下，ログデータ B)．使用する IOC は 6.2 節で述べる．

(2) 部分文字列の抽出

© 2018 Information Processing Society of Japan

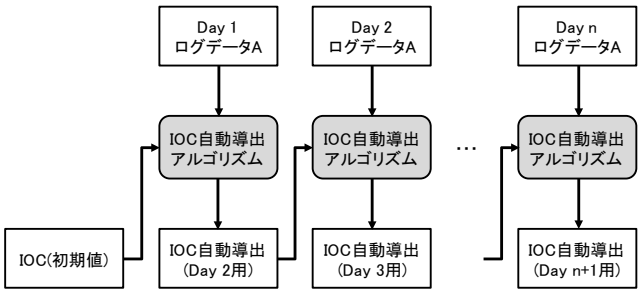

図 8　IOC 自動導出アルゴリズム

Figure 8　IOC auto- derivation algorithm.

表 2　ホワイトリストとして登録した期間

Table 2　Registered period as whitelist.

登録期間	2017/6/1-2017/6/7
登録日数	7 日間
登録データ項目	ドメイン名
データ数(ユニーク数)	2,605,390

表 3　実験期間

Table 3　The duration of the experiment.

実験期間	2017/6/9-2017/6/17
実験日数	10 日間

(1)で抽出した全 URL を対象に，IOC の候補となる複数の URL 間で共通する 6 文字の部分文字列を抽出する．部分文字列の長さを 6 文字固定にしたのは，表 1 の IOC パターン 3 以外が全て 6 文字であり，RIG EK の IOC の特徴が 6 文字で表れると推測したためである．図 6 に部分文字列抽出の概念図を示す.

(3) 部分文字列の選出

各部分文字列毎に，次の 2 つの検出数を算出する．

(a) 部分文字列がログデータ A に含まれる数

(b) 部分文字列がログデータ B に含まれる数

(a)の数=(b)の数, 即ち Jaccard 係数が 1 の部分文字列を選出する．部分文字列選出の概念図を図 7 に示す．Jaccard 係数とは，集合 A 及び B があった場合，式(1)で表される集合の類似度を表す係数である．

$$J(A,B) = \frac{|A \cap B|}{|A \cup B|} \quad (1)$$

抽出部分文字列を Jaccard 係数が 1 の部分文字列だけに限定したのは，例えば"http:/"など汎用的に使われる部分文字列は，ログデータ A と B の重複部分以外のログデータ A 部分にも含まれるためである．

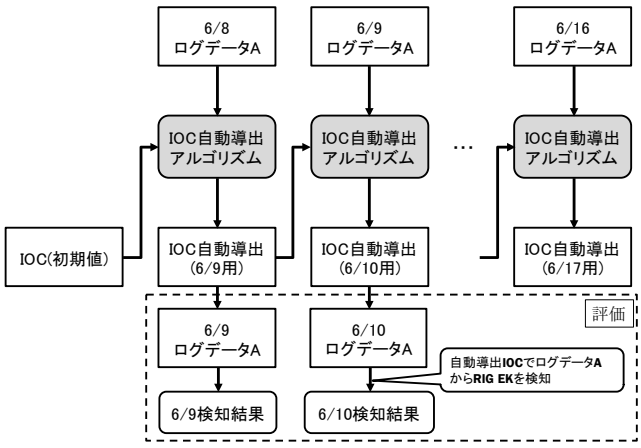

図 9　評価方法

Figure 9　Evaluation method.

6.2 IOC 自動導出アルゴリズムを用いた RIG EK の抽出手法

6.1 節で述べた IOC 自動導出アルゴリズムを用いて RIG EK を抽出する手法の概念図を図 8 に示す.

まず，IOC 初期値を準備する．準備した IOC 初期値は，6.1 節(1)のログデータ B の抽出のために使用する IOC(以下，自動導出 IOC)として用いる.

次に，初日(Day1)のログデータ A に対して IOC 自動導出アルゴリズムにより, 翌日(Day 2)用の IOC を自動導出する．導出した Day2 用の IOC を自動導出 IOC として，Day3 用の自動導出 IOC を導出する．以下，日毎に自動導出 IOC の作成を繰り返す.

自動導出 IOC による RIG EK 抽出の評価結果は，7 章で述べる.

7. 実験と評価

最初に 5 章の前処理手法の評価について述べる.その後，6 章の IOC の自動導出による検知結果を評価する.

7.1 前処理手法の評価

ホワイトリストとして登録した期間,登録したデータ項目,及び登録データ数を表 2 に,実験データとして用いたログデータの期間を表 3 に示す.実験期間は Domain Shadowing のテイクダウン実施前後を含む 10 日間,ホワイトリストの登録期間は実験期間の直前の 7 日間(1 週間)としている.

表 4 に,前処理手法による実験結果を示す.表 3 は,実験期間における,①ログデータ A の数(前処理で抽出したログ数),②ログデータ A に含まれる表 1 のパターンによる検知 URL 数,③ログデータ全体に含まれる表 1 のパターンによる検知 URL 数,及び④カバー率を示す.なお表 1 のパターンは,6/8-6/12 の期間は表 1 のパターン 1-3 を,6/13-6/17 の期間は表 1 のパターン 4-35 を適用して検出している.

表 4 の④のカバー率が平均で 89.7%以上である実験結果

© 2018 Information Processing Society of Japan

表 4　前処理手法の実験結果

Table 4　Experimental results of preprocessing method.

件数,カバー率＼日付	6/8	6/9	6/10	6/11	6/12	6/13	6/14	6/15	6/16	6/17
① ログデータ A の数	3721	5068	4352	4702	5958	6464	6209	7892	7522	10331
②-1 ①に含まれる表 1 のパターン 1-3 による検知数(URL 数)	3	56	141	239	155	0	0	0	0	0
②-2 ①に含まれる表 1 のパターン 4-35 による検知数(URL 数)	0	0	0	0	0	157	25	94	55	155
③ ログデータ全体に含まれる表 1 のパターン 1-35 による検知数(URL 数)	3	58	143	242	155	175	26	95	55	158
④ カバー率((②/③)×100%)	100.0	96.6	98.6	98.8	100.0	89.7	96.2	98.9	100.0	98.1

表 5　実験結果

Table 5　Experimental results.

評価＼日付	6/8	6/9	6/10	6/11	6/12	6/13	6/14	6/15	6/16	6/17
① ログデータ A の数	3721	5068	4352	4702	5958	6464	6209	7892	7522	10331
②-1 ①に含まれる表 1 のパターン 1-3 による検知数(ユニークドメイン数)	-	11	13	14	15	0	0	0	0	0
②-2 ①に含まれる表 1 のパターン 4-35 による検知数(ユニークドメイン数)	-	0	0	0	0	12	9	16	15	19
③ ①に含まれる自動導出 IOC による検知数(ユニークドメイン数)	-	16	15	29	47	30	28	28	36	38
④ ②∩③の検知数(ユニークドメイン数)	-	10	13	14	15	11	9	16	15	19
⑤ 適合率(Precision) $(\frac{②∩③}{③})$	-	62.5	86.7	48.3	31.9	36.7	32.1	57.1	41.7	50.0
⑥ 再現率(Recall) $(\frac{②∩③}{②})$	-	90.1	100.0	100.0	100.0	91.7	100.0	100.0	100.0	100.0

表 6　IOC の自動導出事例

Table 6　Case example of IOC auto-derivation.

xXrQMv
xXvQMv
33Qc_W
3Qc_Wf
3rQc_W
3vQc_W
Qc_WYa
Qc_WZa
Qc_Wfa
rQc_WY
rQc_WZ
vQc_Wf
xXrQMv

は,前処理手法により,RIG EK のログデータが効率良く抽出できていることを示している.

7.2 自動導出 IOC による検知精度の評価

抽出したログデータ A から自動導出 IOC による RIG EK の検知精度について評価する. 評価は,ログデータ A 中に自動導出 IOC を含む URL のドメイン名により行った. IOC 初期値として,表 1 のパターン 1 を用いた.評価方法を図 9 に示す.実験結果は,適合率,再現率で評価を行った.

ログデータ A を用いた RIG EK 検知ユニークドメイン数を表 5 に示す.実験で用いた IOC は, 表 5 の②では表 1 の各パターン、表 5 の③では自動導出 IOC である.表 5 の②は,プライベート IP アドレスを除く IP アドレスをドメイン名に持つ RIG EK のユニークドメイン数をカウントした結果である.本研究では、表 5 の②を RIG EK に適合するドメイン名であると定義し評価を行った.表 5 の③は,自動導出 IOC による検知結果のユニークドメイン数をカウントした結果である.表 5 の④は,②と③に共通するドメイン名をカ

© 2018 Information Processing Society of Japan

ウントした結果である.表 5 の⑤に適合率,⑥に再現率を示す. 表 6 に,6/13 のログデータ A から自動導出した IOC の例を示す. 自動導出 IOC の中に,表 1 のパターンが含まれていることが確認できる.

自動導出 IOC による RIG EK の検知は, 表 5 の⑤から,実験した 9 日間の内,7 日間は RIG EK ドメイン名を 100%,2 日間は 90%以上の再現率(9 日間の平均で約 98%)で検知することができた.一方,適合率は,表 5 の⑥から,9 日間の平均で約 50%であった.実験結果から,提案手法は,定義に適合する RIG EK ドメイン名を平均約 98%で再現(Recall)することができ, 定義に適合する RIG EK ドメイン名に平均約 50%で適合(Precision)する手法であることを確認した.

RIG EK ドメイン名の多くは,Domain Shadowing のテイクダウン前後にドメイン指定から IP アドレス直指定に変化している[21].本研究では,RIG EK の検知結果をより確実に評価するために,IP アドレス直指定のドメイン名だけを RIG EK に適合するドメイン名と定義して評価を行った.しかし,実際は実験結果の中にドメイン指定の RIG EK も存在しており,RIG EK に適合するドメイン名としてカウントしていないために適合率に反映されない結果となった.RIG EK の評価指標の検討は今後の課題である.

8. まとめ

本研究では，あるセキュリティツールの 7 ヶ月間の膨大な長期 Web アクセスログを分析することによって, RIG EK の長期活動を明らかにした．そして，新しい IOC を自動的に導出することにより，RIG EK の IOC の変化に対して頑強な検知方式を提案した．提案方式を評価した結果，RIG EK ドメイン名を平均 98%の再現率，約 50%の適合率で検知できることを確認した．また，自動導出した IOC には既知の IOC を含んでいることを確認しており，期間中の IOC の変化に追従して，新しい IOC を自動導出できることが明らかになった.

謝辞 本研究成果は，国立研究開発法人情報通信研究機構（NICT）の委託研究「Web 媒介型攻撃対策技術の実用化に向けた研究開発」により得られたものです.

参考文献

[1] 森島 周太, 中野 弘樹, 吉岡 克成, 松本 勉, 藤原 礼征, “多数のユーザの Web アクセスログから効率的に悪性サイトを抽出する手法,” コンピュータセキュリティシンポジウム 2017 (CSS2017), 2017.
[2] 山田 道洋, 小池 倫太郎, 菊池 浩明, 黄 緒平, “RIG Exploit Kit における攻撃傾向の調査,” コンピュータセキュリティシンポジウム 2017 (CSS2017), 2017.
[3] 小池 倫太郎, 菊池 浩明, “Drive-by Download 攻撃における RIG Exploit Kit の解析回避手法の調査, ” コンピュータセキュリティシンポジウム 2017 (CSS2017), 2017.
[4] https://blog.trendmicro.com/trendlabs-security-intelligence/a-look-into-recent-exploit-kit-activities/?utm_source=trendlabs-social&utm_medium=smk&utm_campaign=0718_exploit-kits, (参照 2018-08-01).
[5] 西尾 祐哉, 廣友 雅徳, 神薗 雅紀, 福田 洋治, 毛利 公美, 白石 善明, “Exploit Kit で構築された悪性 Web サイトの URL に関する考察,” コンピュータセキュリティシンポジウム 2017 (CSS2017), 2017.
[6] 金子 慧海, トラン フン タオ, 山田 明, 面 和成, “Drive-by Download 攻撃対策に向けた RIG Exploit Kit の決定木分析,” コンピュータセキュリティシンポジウム 2017 (CSS2017), 2017.
[7] 孫 博, 秋山 満昭, 八木 毅, 森 達哉, “既知の悪性 URL 群と類似した特徴を持つ URL の検索,” コンピュータセキュリティシンポジウム 2017 (CSS2017), 2017.
[8] TP. Thao, A. Yamada, K. Murakami, J. Urakawa, Y. Sawaya, A. Kubota, Classification of Landing and Distribution Domains Using Whois’s Text Mining. 2017 IEEE Trustcom/BigDataSE/ICESS.
[9] 秋山満昭, 八木毅, 針生剛男, "改ざん Web サイトリダイレクトに基づく悪性 Web サイトの生存期間測定, " 電子情報通信学会 ICSS 研究会, July 2013.
[10] 嶌田一郎，太田敏史，岡田晃市郎，山田明，“ユーザ環境における RIG Exploit Kit の実態調査方法の提案”，情報処理学会第 78 回コンピュータセキュリティ研究発表会，July 2017.
[11] A. Moshchuk, T. Bragin, S. D. Gribble, and H. M. Levy. "A Crawler-based Study of Spyware on the Web," In Proceedings of the 2006 Network and Distributed System Security Symposium, pages 17–33, February 2006.
[12] N. Provos, D. McNamee, P. Mavrommatis, K. Wang and N. Modadugu, “The ghost in the browser analysis of web-based malware, " In 1st Workshop on Hot Topics in Understanding Botnets, 2007.
[13] N. Provos, P. Mavrommatis, M. A. Rajab and F. Monrose, "All Your iFRAMEs Pointto Us," In Proceedings of the 17th USENIX Security Symposium, USENIX Security, 2008.
[14] 松中隆, 窪田歩, 星澤裕二, "Drive-by Download 攻撃対策フレームワークにおける Web アクセスログを用いた Web リンク構造の解析による悪性サイト検出手法の提案," コンピュータセキュリティシンポジウム 2014, October 2014.
[15] 松中隆, 山田明, 窪田歩, "ユーザ参加型 Web セキュリティ観測システムにおける収集情報の網羅性に関する一考察," コンピュータセキュリティシンポジウム 2015, October 2015.
[16] 株式会社 LAC, “猛威を振るう RIG Exploit Kit の全貌と対策”, CYBER GRID VIEW Vol.3, https://www.lac.co.jp/lacwatch/report/20170202_001203.html, (参照 2018-08-01).
[17] “2017 - **NEW**UPDATED** Rig Exploit Kit malware URL Patterns June 12 - Current Date (November 1st, 2017) | Part 3”. https://www.linkedin.com/pulse/2017-new-rig-exploit-kit-malware-url-patterns-june-14-baber/, (参照 2017-12-14).
[18] “SHADOWFALL”. https://www.rsa.com/en-us/blog/2017-06/shadowfall, (参照 2018-08-01).
[19] https://www.paterva.com/web7/index.php, (参照 2018-08-03)
[20] https://www.godaddy.com, (参照 2018-08-03)
[21] https://www.jpcert.or.jp/present/2018/JSAC2018_05_ikuse.pdf, (参照 2018-08-20)

© 2018 Information Processing Society of Japan