URLを分割する難読化が施された悪性JavaScriptの検出法

情報工学科　笹瀬研究室　森重翔也

研究背景

ドライブバイダウンロード攻撃に使用される悪性JavaScriptには難読化が施され，既存のウイルス対策ソフトでは検知困難である．

└→ 文字列の変換処理により可読性を低下させる手法
例）エンコード難読化（**図1**）

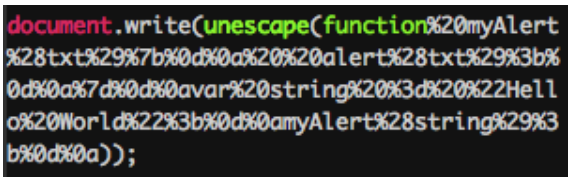

図1 エンコード難読化

従来方式

エンコード難読化の多用によるコード内の文字出現頻度の変化に着目し，それを特徴量とした機械学習により悪性JavaScriptを検知する．

問題点

悪性ウェブサイトのURLを分割することでパターンマッチングを回避するJavaScriptが複数存在した．（**図2**）

文字出現頻度が良性と似ているため検出困難

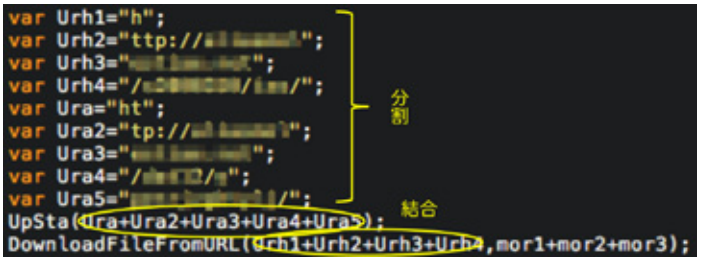

図2 URL分割型の難読化JavaScript

提案方式

URLの断片は変数に代入されたのちに文字列として結合されることに着目

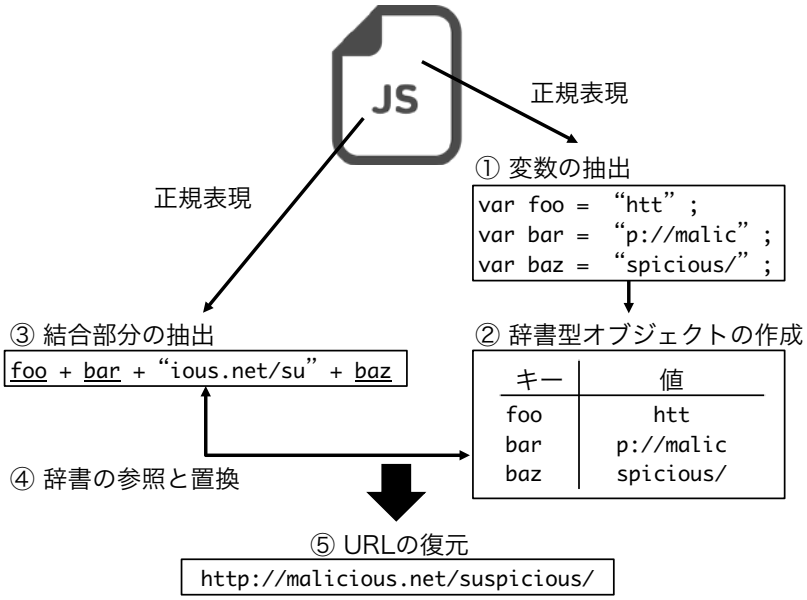

図3 提案方式のアーキテクチャ

- 変数名と中身を辞書型オブジェクトに保存
- 結合部分の文字列を辞書のキーと参照して置換
- URLが復元された場合に悪性に分類

特性評価

良性JavaScript：2,338ファイル
悪性JavaScript：3,247ファイル
に対する検知精度を比較

表1 検知精度の比較

	従来方式	提案方式
False Positive	31ファイル	31ファイル
False Negative	61ファイル	49ファイル
正答率	96.67%	97.11%

提案方式は
FPを増加させることなくFNを20%削減可能

結論

本研究では，URLを分割する難読化が施された悪性JavaScriptに対し，URLの復元を確認する検知方式を提案し，従来方式の検知精度を改善可能であることを示した．

本研究に関する業績

[1] 森重翔也, 春田秀一郎, 朝比奈啓, 笹瀬巌, "URLを分割する難読化が施された悪性JavaScriptの検出法, "電子情報通信学会通信方式研究会, vol. 117, no. 156, CS2017-15, pp. 13-18, 2017年7月27日.
[2] Shoya Morishige, Shuichiro Haruta, Hiromu Asahina, and Iwao Sasase, "Obfuscated Malicious JavaScript Detection Scheme Using the Feature Based on Divided URL", The 23rd Asia-Pacific Conference on Communications (APCC), Perth, Australia, 11-13, December 2017.

宛先までのホップ数解析によるTracerouteを用いたTarget Link Flooding Attack検知手法

情報工学科　笹瀬研究室　佐久間慧

研究背景

近年，新種のDDoS攻撃であるTarget Link Flooding Attack が報告されている

Target Link Flooding Attackとは…
- ターゲットへ直接パケットを送信しないDDoS攻撃
- 特定のリンクを輻輳させることでターゲットをネットワークから孤立させることが目的

従来のDDoS攻撃に対する対策が適用困難

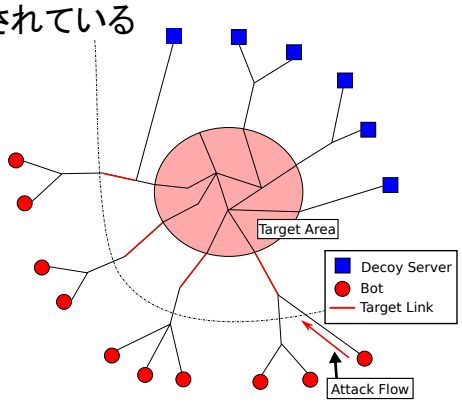

図1: Target Link Flooding Attackの例

従来手法

Tracerouteの増加による攻撃の予兆を検知

- 攻撃者は，ネットワークトポロジーを把握するために大量のボットからTracerouteを送信する必要有
- 攻撃者によるTracerouteが正規のユーザによるものと混同してしまった場合，検知不可能になる可能性

提案手法

宛先までのホップ数解析により攻撃の予兆を検知

- 攻撃の準備に用いられるTracerouteの宛先はターゲットリンク付近に集中
- Traceruteを宛先までのホップ数毎に分類
- ホップ数毎に解析することで従来よりも変化が強調され，攻撃の予兆を捉えやすく

特性評価

- インターネットの形状を模したデータセットで検知精度を評価
- AUCを用いて評価(1に近いほど良い検知精度)
- ノイズ(正規のユーザーによるTraceroute)が増えた場合に攻撃を検知可能かを評価
- ノイズが増えた場合でも，従来手法に比べ十分に検知可能

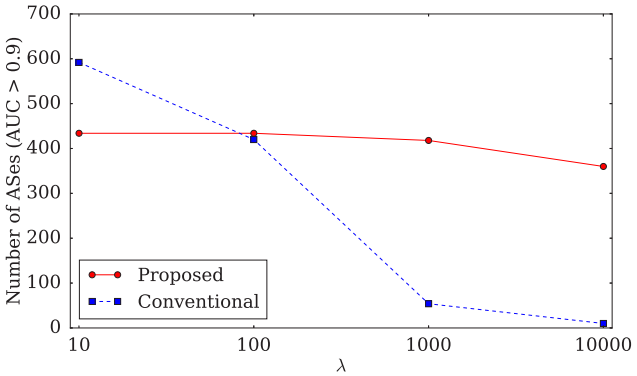

図2: ノイズに対する高AUCを記録したASの数の変化

本研究に関する業績

1. 佐久間慧, 朝比奈啓, 春田秀一郎, 笹瀬巌、"宛先までのホップ数解析によるTracerouteを用いたTarget Link Flooding Attack検知手法," 電子情報通信学会通信方式研究会, 2017年11月16日.
2. Kei Sakuma, Hiromu Asahina, Shuichiro Haruta, and Iwao Sasase, "Traceroute-based Target Link Flooding Attack Detection Scheme by Analyzing Hop Count to the Destination," The 23rd Asia-Pacific Conference on Communications (APCC), Perth, Australia, 11-13, December 2017.