セキュアシステム開発実験
IDS フリーソフトによる不正トラフィックの検知

2600190179-5 菅原颯真
H チーム

2021 年 7 月 31 日

目次

1　テーマ概要

情報通信が日常に欠かせないものとなったいま，日々多くの通信が行われているが中には不正なトラフィックがあることも事実である．

本実験では IDS と呼ばれる不正侵入検知システムのフリーソフトである「zeek」を用いて通信トラフィックを調査し，どのようなトラフィックが不正なトラフィックであるかを調査するとともに，実際に不正なトラフィックを流した時の検知の様子を調査する．

2　実行環境

今回，実験を行った時の実行環境および使用ツールについて以下に示す．また，図示したものを図 1 に示す．

- ホスト OS：macOS BigSur 11.4 (64bit)
- ゲスト OS：ubuntu 18.04 (64bit)
- OS 仮想化ソフトウェア： Parallels Desktop 16 for Mac
- ネットワーク分析フレームワーク：Zeek (v4.0.1)

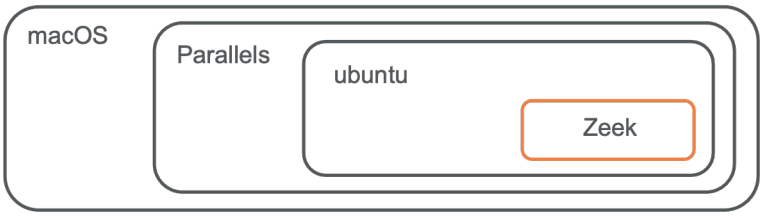

図 1　実行環境

3　zeek の仕組み

zeek の仕組みは図 2 に示す通り，ネットワークトラフィックをイベントエンジンコンポーネントに取り込む．パケット解析では，リンク層から始まる低レベルのプロトコルを処理する。セッション解析では，HTTP や FTP などのアプリケーション層のプロトコルを処理する。ファイル解析は，セッションで転送されたファイルの内容を解析する．解析した結果をポリシースクリプトインタープリターに渡して結果に応じてログや通知を出力する．pcap ファイルを渡すことで擬似的にパケットを解析し，ログを生成することを実現できる．

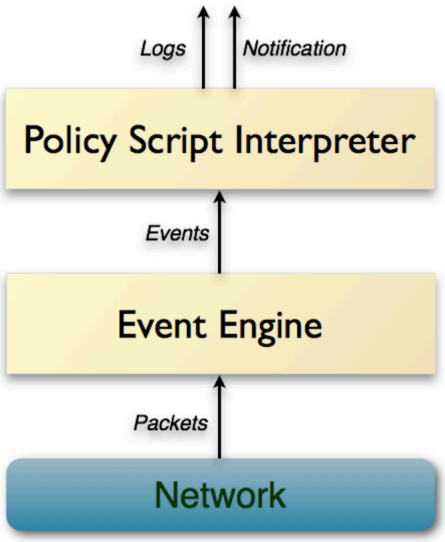

図 2　zeek の仕組み

4　実験経過

実験開始時は図のように自ら内部ネットワークに不正なトラフィックを流して検出および log の保存を行おうと考えたが，内部ネットワークに不正なトラフィックを流すためにはサーバーを作成する必要があり当時の技術力および時間の関係から不可能であると判断した．

そのため，実際にマルウェアとの通信をキャプチャした有害な pcap ファイルを公開している `https://www.malware-traffic-analysis.net/` というサイトがあったため，そこから pcap ファイルをダウンロードし，不正トラフィックが Zeek を通ったと仮定して log を分析する．

5　log の解析

ここでは，log の解析および被害を受けた過程の考察を行う．今回は 2020 年に被害が確認された Lokibot の pcap ファイルの解析を行った．ちなみに，Lokibot はトロイの木馬型のマルウェアである．
解析の流れは以下の通りである．

- Zeek をオフラインモードで起動
- 指定の pcap ファイルをロード（今回は Likibot の pcap ファイル）
- pcap ファイルから得たトラフィックの log を解析
- どのようにしてマルウェアに感染したのかを調べる

5.1　オフラインモードで起動・ロード

オフラインモードでの起動・ロードは”zeek -r （解析対象のファイル）”を実行することで可能となる．今回の解析対象ファイルは 2020-10-12-Lokibot-infection-traffic.pcap のため，”zeek -r 2020-10-12-Lokibot-infection-traffic.pcap”を実行した．

5.2　log の解析

まず，取得できた log は以下の通りである．

logの種類	概要	logの種類	概要
conn.log	TCP / UDP / ICMP接続	packet_filter.log	適用されたパケットフィルタの一覧
dns.log	DNSアクティビティ	pe.log	Portable Executable（後述）
files.log	ファイルの分析結果	ssl.log	SSL/TLSハンドシェイク情報
http.log	HTTPリクエストと応答	x509.log	X509証明書情報

図 3　log の一覧表

6　感染経路の考察

まず，マルウェアに感染していることから何らかの実行形式のファイルがダウンロードされている可能性が高い．log の一覧を見てみると Portable Executable（Windows の 32 ビット（64 ビット）の実行可能なファイル形式（EXE）のこと）に関する pe.log という log が怪しそうなので，見てみると該当するトラフィックが一件見つかった．

```
#fields ts      id      machine compile_ts      os      subsystem       is_exe
#types  time    string  string  time    string  string  bool    bool    bool
1602536538.738140       FkmfCx13mub2PIRUO7      I386    708992537.000000
```

図 4　pe.log の一部

このトラフィックの ID はすべての log で共通の ID として利用されているため，今度はこの ID からすべての log を検索する．検索した結果を以下に示す．

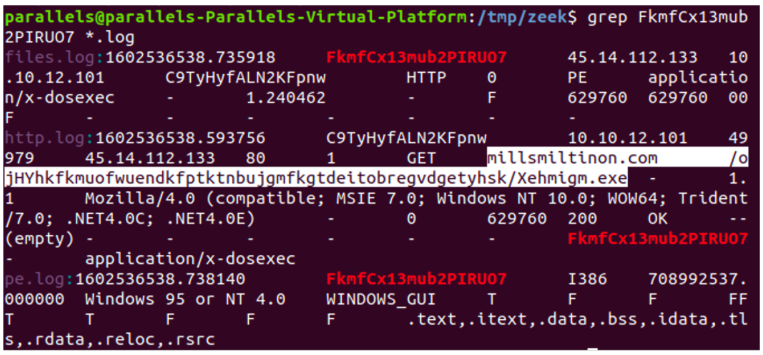

図 5　ID の検索結果

これをみると怪しいサイトから怪しいファイルがダウンロードされていることがわかり，このサイトを訪れた際に感染した可能性が高いと考える．先程の ID を用いて http.log を調べると

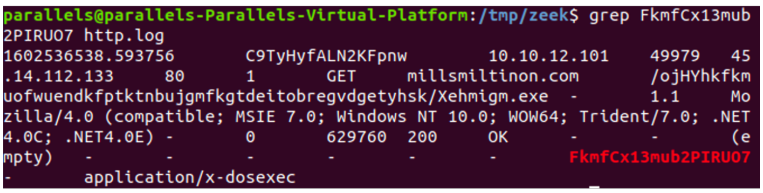

図 6　http.log

送信元 IP アドレスおよびポート番号がわかり，どこから感染したかが明確化された．このような手法で感染の経緯を分析し以降，この IP アドレスおよびポート番号からの通信をシャットアウトすることで今後のマルウェア感染を防ぐことができる．

7　まとめ

元々目標としていた zeek によるシグネチャの作成および不正トラフィックの検出・通知はできなかったが，IDS に仕組みについての理解が深まった．また，どのような流れで log を生成しているのかも確認できた．擬似的にトラフィックの解析，および不正トラフィックの調査を行うことができ，実際にどのような形で感染被害にあったのかの調査がどれだけ大変かを実感することができた．ただ，このような調査に対しての興味が深まったので今後，個人的に勉強していきたい．また，元々目標としていた zeek によるシグネチャの作成および不正トラフィックの検出・通知にも挑戦してみたい．

参考文献

[1] Zeek Documentation, https://docs.zeek.org/en/lts/index.html#
[2] IPA, ネットワークセキュリティに関する知識 II, https://www.ipa.go.jp/files/000056339.pdf