報道各位

2018年8月17日
株式会社インプレスR&D
https://nextpublishing.jp/

“おもてなし”機能でサイバー攻撃を観察する！

『WOWHoneypotの遊びかた』発行

技術書典シリーズ、8月の新刊

インプレスグループで電子出版事業を手がける株式会社インプレスR&Dは、『WOWHoneypotの遊びかた』(著者:森久和昭)を発行いたします。

『WOWHoneypotの遊びかた』
https://nextpublishing.jp/isbn/9784844398394

著者:森久 和昭
小売希望価格:電子書籍版 1600円(税別)／印刷書籍版 1800円(税別)
電子書籍版フォーマット:EPUB3／Kindle Format8
印刷書籍版仕様:B5判／カラー／本文102ページ
ISBN:978-4-8443-9839-4
発行:インプレスR&D

＜＜発行主旨・内容紹介＞＞

【ハニーポットを実際に運用して、サイバー攻撃の実態を目の当たりにしてみよう！】

本書はセキュリティ技術の一つであるハニーポットの中でも、サイバー攻撃への対応に優れた著者開発の「WOWHoneypot(Welcome to Omotenashi Web Honeypot)」の解説書です。ハニーポットとは、あえてサイバー攻撃を受けることを前提としたシステムで、リアルな攻撃を解析することができます。

〈本書の対象読者〉

セキュリティに興味がある人
ハニーポットを運用してみたい人
ハニーポットのログ分析のノウハウを知りたい人

(本書は、次世代出版メソッド「NextPublishing」を使用し、出版されています。)

一般的なハニーポット技術の解説と、WOWHoneypot の特徴を紹介

HTTP レスポンスステータスコード[2]を表 1-4 に示します。

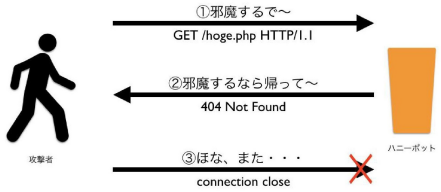
表 1-4 代表的な HTTP レスポンスステータスコード

ステータスコード	意味
200 OK	リクエストが成功したことを示す。
201 Created	ファイルが作成できたことを示す。PUT リクエスト。
401 Unauthorized	認証が必要なページへのアクセスを示す。
403 Forbidden	アクセス権がなく、閲覧できなかったことを示す。
404 Not Found	アクセスしたファイルが存在しなかったことを示す。
405 Method Not Allowed	指定したメソッドが許可されなかったことを示す。
500 Internal Server Error	サーバー側でエラーが発生したことを示す。
501 Not Implemented	指定したメソッドがサポートされていないことを示す。

攻撃者が使う攻撃ツールは、無数に存在します。その中でもしっかりと作り込まれているものは、攻撃対象の状態を見極める機能が備わっています。もっとも初歩的なロジックとしては、アクセス対象のファイルが存在しない場合は、その時点で攻撃ツールを停止させるというものです。ファイルが存在しないにも関わらず攻撃の段階を進めても効果が無く、攻撃者にとって効率的ではありません。そこで攻撃する価値があるのかどうかを評価し、見極めているのです。

図 1-4 は一般的な Web ハニーポット[3]の動作を表したものです。攻撃者が hoge.php に対してアクセスした際に、ハニーポットからそのようなファイルは存在しないという 404 Not Found というステータスコードを返すと、通信を切断してしまいます。結局ハニーポットは、攻撃者の意図を分析する材料が少なくなります。

図 1-4　一般的な Web ハニーポットの動作

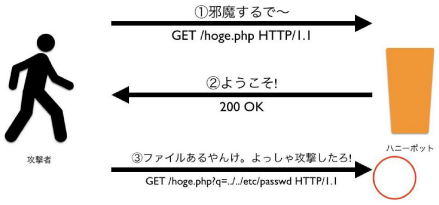


2 https://developer.mozilla.org/ja/docs/Web/HTTP/Status
3 高対話型・低対話型の両方を含む。

WOWHoneypot は、このような攻撃ツールの対策として、とりあえずファイルが存在するようにみせかける 200 OK を返します。そうすることで、攻撃ツールにあえて攻撃段階を進ませて、攻撃を観測するという特徴を持っています。

図 1-5 は WOWHoneypot の動作を表したものです。攻撃者が hoge.php に対してアクセスした際に、とりあえず 200 OK というステータスコードを返します。すると攻撃者は攻撃対象のファイルが存在すると認識して、攻撃の段階を進め、ディレクトリトラバーサルを用いたパスワードファイル閲覧を試みる攻撃を仕掛けてきました。つまり攻撃者の狙いは機密情報の不正な取得であると分析することができます。

図 1-5　WOWHoneypot の 2000K を返す動作



WOWHoneypot であれば、(1)と(3)の要求内容をログとして記録することができ、ハニーポッターがログ分析をするときの情報源が増えるため、攻撃者の狙いをつまびらかにしやすくなります。

特徴 4：マッチ&レスポンス

マッチ&レスポンスは WOWHoneypot の最も重要な特徴で、攻撃者をおもてなしするための工夫です。端的に説明すると「攻撃者からの要求内容に、事前に定義した文字列が含まれていたら、特別な内容を応答する」という機能です。いわゆる IDS(Intrusion Detection System：侵入検知システム)や WAF(Web Application Firewall：Web アプリケーションファイアウォール)のルールベースのシグネチャを作ることができ、条件に一致した場合は、応答内容に細工を施します。

なぜこのような機能が必要かというと、デフォルト 200 OK の説明で触れたツールよりも、さらに一歩進んだ”賢い”攻撃ツールが存在するからです。セキュリティ診断や、脆弱性検証

ログ分析の事例から、最新のサイバー攻撃の実態を紹介

第4章　ログ分析の参考事例

本章では、WOWHoneypot を使った分析の事例を紹介します。ハニーポッターにとって、ログ分析は一番楽しく、また難しいものです。ハニーポットを始めたばかりだと、どのように分析すればいいのか頭を悩ませると思います。そのときには、本章を参考にしてみてください。そしてあなたなりの分析手法を見つけてください。

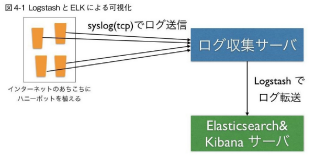
第 1 節　Logstash&ELK による可視化

第 1 項　ログを俯瞰する仕組み

WOWHoneypot で得たログは目的に合わせて分析をしていただきたいのですが、まずはどういった検知傾向にあるのか概要をつかみたい場合があると思います。このような場合には Logstash と ELK(Elasticsearch+Kibana)を組み合わせた可視化をしてみてはいかがでしょうか。可視化といえば、T-Pot と呼ばれるハニーポットを使用している方は、Web の管理画面でグラフや検知傾向を見たことがあるのではないでしょうか。それに対し、WOWHoneypot には標準で可視化する機能は用意されていないので、独自に作成する必要があります。

今回の構成は、複数の WOWHoneypot をインターネットのあっちこっちに植えて、Syslog でログを収集し、1 つのサーバーに集約することとします。さらに Logstash を使って、ログ収集サーバーからログを読み取り、検索システムである Elasticsearch に転送します。最後に Kibana が Elasticsearch のデータを可視化します。その結果、検知傾向をブラウザーから視覚的にわかりやすくなります。構成のイメージを図 4-1 に示します。

図 4-1 Logstash と ELK による可視化



第 2 項　可視化サンプル

Kibana で検知傾向を可視化したサンプルを次の図 4-2、図 4-3、図 4-4 に示します。

図 4-2 は、複数の検知状況をまとめたダッシュボードの例です。mrrid のルールに一致した件数や、ハニーポットごとに検知した件数、宛先ポート番号の件数を上段に据えています。下段には、メソッドの割合、HTTP バージョンの割合、ログの検知件数を表示しています。このようなダッシュボードを用意しておくことで、WOWHoneypot がどのようなログを記録しているのか、おおよその見当がつきます。たとえば POST メソッドや PUT メソッドが割合的に多いと、攻撃者からのデータ送信やファイルアップロードが多い傾向にあることがわかります。その他にルール毎の件数を把握しておくことにより、どの攻撃が多かったのかが見た目で把握しやすいです。

図 4-2 ダッシュボードの例

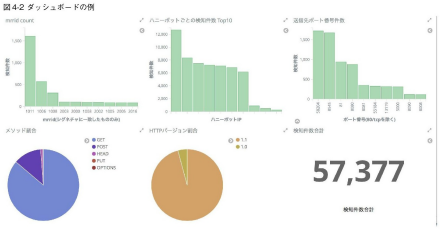


図 4-3 は国別の検知件数をヒートマップにした図です。色が濃いほど、多くのログを検知したことを示しています。今回は国でまとめていますが、都市でまとめるとより具体的な送信元を把握しやすくなります。なお日本の色が濃くなっていますが、これは筆者による WOWHoneypot の死活監視用のリクエストが含まれているためです。

実際に WOWHoneypot で収集できたマルウェア情報なども豊富に掲載

ハンティング機能とchase-url.pyを連携して使うことで、どれだけの不審なURL情報を収集することができたのか実例を紹介します。最初にVirusTotalのAPIの使用状況を次の図4-23に示します。筆者のハニーポット環境において、2018年5月6日から6月12日まで1ヶ月強の期間のAPI使用状況です。

図4-23 chase-url.pyによる調査状況

APIを利用した調査回数は、最多でも1日に90回程度でした。また日によって、ほとんど調査しないこともあり、大きな波があることがわかります。なおここではAPIの使用回数を数え上げているだけです。つまりハッシュ値の検索と、サブミットした回数の両方が含まれています。実際のところ、VirusTotalで未解析のファイルは少なく、サブミットする頻度は1日に数件程度です。それでも、この数件は世界でも知られていない可能性があるファイルであり、サイバー攻撃の最先端を分析していることに変わりはありません。

次にVirusTotalへサブミットされたファイルを3つ紹介します。図4-24はサンプル1です[15]。Comodoの検出名である「Packed.Win32.MUPX.Gen」や、VirusTotalのファイルの詳細情報から得られる情報より、UPXでパックされたWindows環境で動作する実行形式のファイルです。パックとは、攻撃者が使う常套手段の1つで、セキュリティ技術者が容易にマルウェア解析させないようにする場合や、セキュリティ対策製品で検知されないようにする場合などに使われる技術です。今回の結果から、アンチウイルスソフトの検出名からは、具体的に何のマルウェアであるかという情報は得られません。詳細なマルウェアの情報を知るために、アンパックして解析する必要があります。パックやアンパックについては、本書の趣旨から外れる内容のため割愛します。

15.https://www.virustotal.com/ja/file/e96b64acf4c98da4d6c3964343b38cc808868282923e680371a084cb725b7bad7e/analysis/

図4-24 ハンティング機能で得たマルウェア情報のサンプル1

BitDefender	Gen:Variant.Zusy.289785
Bkav	W32.eHeur.Malware14
Comodo	Packed.Win32.MUPX.Gen
CrowdStrike Falcon (ML)	malicious_confidence_100% (W)
Cylance	Unsafe
Cyren	W32/Dialer.B.gen!Eldorado

次に別のファイルのサンプル2を図4-25に示します[16]。各アンチウイルスソフトの検出名から、明らかにPerlで作られたボットプログラムであると予想がつきます。おそらく脆弱性を悪用して、このPerlプログラムをWebサーバーにダウンロードおよび実行させて、ボットの一部として取り込むために使われた可能性が考えられます。

図4-25 ハンティング機能で得たマルウェア情報のサンプル2

ESET-NOD32	Perl/Shellbot.NAL.Gen
F-Prot	Unix/ShellBot.AA
F-Secure	Backdoor.Perl.Shellbot.B
Fortinet	Perl/ShellBot.NAK!tr
GData	Backdoor.Perl.Shellbot.B

最後に3つ目のサンプルを図4-25に示します[17]。Kasperskyの検知名「HEUR:Backdoor.Linux.Ganiw.d」から、Linux環境で動作するGaniwマルウェアと考えられます。Ganiwマルウェアは、DDoS攻撃の踏み台として使われることが知られています。

セキュリティに関する情報収集をしていると、頻繁にDDoS攻撃の被害を受けたというニュー

16.https://www.virustotal.com/ja/file/81fb35e7189e9bf87197a042f84e0b8f0db63b32b99b04726c0dfbab59000159f/analysis/
17.https://www.virustotal.com/ja/file/1e1810b52103a5a3d63ada1fcb853e2e5c88d08d5ce6d44e6b18beaf76a1f80e/analysis/

＜＜目次＞＞

第1章　一般的なハニーポットとWOWHoneypot
1　概要
2　ハニーポットの分類
3　WOWHoneypotとは
4　WOWHoneypotの概要と特徴
5　WOWHoneypotで捉えられない攻撃
第2章　WOWHoneypotを植えてみる
1　Digital Oceanで環境準備
2　WOWHoneypotインストール
3　設定
4　動作確認
第3章　マッチ&レスポンスルール詳解
1　項目解説
2　作成例
3　動作検証
第4章　ログ分析の参考事例
1　Logstash&ELKによる可視化
2　アクセス先のパスを眺める
3　公開情報を元にハニーポットのログ調査
4　最新のサイバー攻撃を追いかける
5　マルウェア情報ハンティング
6　ハニーポットを脆弱性の理解に使う

7　Drupalgeddon2 で見る低対話型と高対話型の比較
8　特定のテーマでログを分析する　仮想通貨編

＜＜著者紹介＞＞

森久 和昭
インターネットの隅っこで、ハニーポットを運用するハニーポッターとして活動している。ブログ（https://www.morihi-soc.net/）にハニーポットの構築方法や、ログ分析した結果をハニーポット観察記録として公開、その他セキュリティに関する記事を公開している。本業はネットワーク・セキュリティエンジニア・アナリスト。著書に「サイバー攻撃の足跡を分析するハニーポット観察記録」（秀和システム）がある。

＜＜販売ストア＞＞

電子書籍:
Amazon Kindle ストア、楽天 kobo イーブックストア、Apple iBookstore、紀伊國屋書店 Kinoppy、Google Play Store、honto 電子書籍ストア、Sony Reader Store、BookLive!、BOOK☆WALKER
印刷書籍:
Amazon.co.jp、三省堂書店オンデマンド、honto ネットストア、楽天ブックス
※　各ストアでの販売は準備が整いしだい開始されます。
※　全国の一般書店からもご注文いただけます。

【株式会社インプレス R&D】 https://nextpublishing.jp/
株式会社インプレスR&D（本社:東京都千代田区、代表取締役社長:井芹昌信）は、デジタルファーストの次世代型電子出版プラットフォーム「NextPublishing」を運営する企業です。また自らも、NextPublishing を使った「インターネット白書」の出版など IT 関連メディア事業を展開しています。
※NextPublishing は、インプレス R&D が開発した電子出版プラットフォーム（またはメソッド）の名称です。電子書籍と印刷書籍の同時制作、プリント・オンデマンド（POD）による品切れ解消などの伝統的出版の課題を解決しています。これにより、伝統的出版では経済的に困難な多品種少部数の出版を可能にし、優秀な個人や組織が持つ多様な知の流通を目指しています。

【インプレスグループ】 https://www.impressholdings.com/
株式会社インプレスホールディングス（本社:東京都千代田区、代表取締役:唐島夏生、証券コード:東証 1 部 9479）を持株会社とするメディアグループ。「IT」「音楽」「デザイン」「山岳・自然」「旅・鉄道」「学術・理工学」を主要テーマに専門性の高いメデイア&サービスおよびソリューション事業を展開しています。さらに、コンテンツビジネスのプラットフォーム開発・運営も手がけています。

【お問い合わせ先】

株式会社インプレス R&D NextPublishing センター
TEL 03-6837-4820
電子メール: np-info@impress.co.jp