Vol.2022-CSEC-97 No.22
Vol.2022-IOT-57 No.22
2022/5/20

ハニーポットによる攻撃観測と多角的分析のための統合アーキテクチャの提案

佐々木貴之[1]　九鬼琉[2]　植田岳洋[3]　鮫嶋海地[3]
Guo Binnan[3]　市川詩恩[2]　山口陽平[2]
岡田 晃市郎[4]　吉岡 克成[5]　松本 勉[5]

概要：IoT 機器を対象としたサイバー攻撃の動向を明らかにするために，IoT 機器を模倣したハニーポットを運用しており，2021 年は 1 年間で約 4 千万件のスキャンや攻撃を観測し，のべ 8 千を超えるマルウェア検体を収集した．サイバー攻撃の実態把握のために，これらの観測データを解析し，攻撃の対象となっている機器や脆弱性を明らかにしたい．加えて，攻撃元の振る舞いや，脆弱性の悪用のされ方を分析することができれば，攻撃の背景が明らかになる．さらに，観測データから未知の攻撃を発見できれば，迅速な対策の実施に繋がる．これらを実現するためには，ハニーポットで観測した大量のデータや収集した多様な検体を効率的に解析する必要がある．そこで，ハニーポット，動的解析，ルールベースの攻撃タグ付けを組み合わせ，攻撃観測と分析を統合したアーキテクチャを提案する．本アーキテクチャの特徴は，(1) ハニーポットで収集した検体を自動的に動的解析し，疑似インターネットとの通信を観測することにより，マルウェアが行う攻撃を抽出する点と，(2)ハニーポットで観測した攻撃や，検体の動的解析で観測した攻撃について，ルールに基づいて自動的に CVE 番号や攻撃対象機器をタグ付けする点にある．プロトタイプを実装し評価実験を行った結果，50 件を超える脆弱性を狙う攻撃がハニーポットで観測されていることが明らかになった．加えて，動的解析中にマルウェアが行った攻撃の対象の CVE とハニーポットで観測された攻撃対象の CVE の関係を分析したところ，動的解析で観測した攻撃の 85%はハニーポットでも観測されていた．

キーワード：ハニーポット，セキュリティ，IoT，攻撃解析

Integrated Architecture for Honeypot Observation and Multi-purpose Analysis

Takayuki Sasaki[1]　Ryu Kuki[2]　Takahiro Ueda[3]　Kaichi Sameshima[3]
Binnan Guo[3]　Shion Ichikawa[2]　Youhei Yamaguchi[2]
Kouichirou Okada[4] Katsunari Yoshioka[5] Tsutomu Matsumoto[5]

Abstract:
We have operated honeypots to observe cyberattacks against IoT devices and observed 40M accesses and over 8K malware samples in 2021. The goals of the observation are the identification of target devices and vulnerabilities. In addition, understanding attackers' behaviors and misuse of the vulnerabilities is another goal to deploy adequate measures. Furthermore, if we can find zero-day vulnerabilities from the attacks, quick responses against the attacks can be realized. Towards these goals, we propose an architecture comprising honeypots, dynamic analysis, and rule-based attack tagging. Features of the architecture are (1) extracting attacks from malware using dynamic analysis and (2) tagging attacks observed by the honeypots and dynamic analysis based on pre-defined rules. We implemented a prototype of the architecture and identified that our honeypot observed over 50 types of attacks. Moreover, we investigated the attacks observed by honeypots and dynamic analysis and identified that CVEs observed by honeypots include 85% of CVEs observed by the dynamic analysis.

Keywords: Honeypot, Security, IoT, Attack analysis

1. はじめに

IoT(Internet of Things)の発展に伴い，IoT 機器を対象としたサイバー攻撃が活発化している[1][2]．我々は，このようなサイバー攻撃を観測するために，IoT 機器の WebUI を模倣したハニーポット(X-POT)[3]を運用しており，1 年間のアクセスが約 4 千万件と膨大な数のスキャンや攻撃が観測されている．

ハニーポットで得た観測データを分析する際の目標は，どのような攻撃がいつ行われているかの可視化と，未知の脆弱性を利用した攻撃のいち早い発見である．加えて，攻撃元の振る舞いや，脆弱性の悪用のされ方を分析することができれば，攻撃の背景が明らかになる．さらに，観測データから未知の攻撃を発見できれば，迅速な対策の実施に繋がる．これらの目標の達成のためには，分析対象のデー

1 横浜国立大学先端科学高等研究院
2 横浜国立大学理工学部 数物・電子情報系学科
3 横浜国立大学大学院 環境情報学府
4 横浜国立大学先端科学高等研究院/レインフォレスト
5 横浜国立大学大学院環境情報研究院/先端科学高等研究院

ⓒ2022 Information Processing Society of Japan

タの最大化と，大量のデータの効率的な分析の 2 点を実現する必要がある．

分析対象のデータの最大化に関して，提案アーキテクチャでは，ハニーポットで直接観測したデータに加えて，動的解析で得た通信データも解析の対象とする．なぜなら，マルウェアによっては，内部に複数の攻撃コードを持ち，感染したコンピュータからその機能を用いて感染を拡大させるマルウェア[7]が報告されているためである．ハニーポットで収集したマルウェアを解析し，その内部に存在する攻撃コードを調べることで，攻撃のトレンドのより良い理解や未知の攻撃を発見するチャンスを増やすことができる．加えて, ハニーポットの観測データと組み合わせることで，IoT 機器の Exploit，マルウェアの侵入，再攻撃という一連の攻撃の内容を明らかにできる可能性がある．

データの分析に関して，攻撃のトレンドの分析や未知の攻撃を発見しようとすると，ハニーポットの大量の観測データから攻撃を抽出し，それぞれの攻撃に対して既知の攻撃か未知の攻撃か，既知の攻撃であれば CVE 番号などの情報をタグ付けする必要がある. しかし, 前述したように，ハニーポットで観測されるイベントは膨大であるため，手作業では分析が不可能であり, 自動化が必須である. また，日々新しい攻撃が現れる現状を鑑みると，前述した攻撃のタグ付けのためのルールについても自動的に生成されることが望ましい．

本論文では，ハニーポットで観測したデータを効率的に分析するアーキテクチャを提案する. 本アーキテクチャは，ハニーポット，ハニーポットで収集したマルウェアを自動的に動的解析して Exploit を抽出する動的解析コンポーネント，攻撃に対してタグ付けを行うコンポーネントから構成される．本アーキテクチャの特徴は，ハニーポットで収集した検体に対して自動的に動的解析を行い，マルウェアの感染拡大活動も解析の対象とすることで，解析するデータの最大化を図っている．さらに，ハニーポットで直接得られた攻撃リクエストと，上述した動的解析で得られた攻撃リクエストに対して，感染に利用する脆弱性や攻撃対象の機器を自動的にタグづけることで，解析の効率化を行っている．

提案アーキテクチャを実装し 2021 年 1 月から 2022 年 2 月のデータを解析した結果，ハニーポットによって 50 種類の攻撃が観測された．また，ハニーポットと動的解析で観測した攻撃は，両方とも古い脆弱性から新しい脆弱性まで幅広く利用していた．

以上を整理すると，本論文の貢献は以下の点である．

- ハニーポットで観測した攻撃やマルウェア検体を解析するためのアーキテクチャ設計と実装
- ハニーポットで観測したデータと動的解析で検体から抽出した Exploit の攻撃タグ付けによる分析

2. 関連研究

ハニーポット：ハニーポットとは脆弱なシステムを模倣し，攻撃を誘引することで観測を行うシステムである．その一つとして，インターネットから攻撃対象となっている機器の応答を収集し，模倣する機器を拡張可能な HTTP ハニーポットである X-POT[1]が提案されている. X-POT は，特定パスに複数の IP アドレスからアクセスがあった際に，そのパスを持つ機器が新しい攻撃対象となっていると仮定する．そして，そのパスにアクセスした IP アドレスの周辺を探索し，そのパスを持つ機器が発見できた場合に，その応答(WebUI の HTML)を取得する．具体的には，特定のパスに閾値以上の回数のアクセスがあった際に，それをトリガーとして，スキャンと応答の取得を行うように実装されている．このように，インターネットから機器の応答を取り込むことで，模倣する機器を拡張することができる．提案アーキテクチャでは，攻撃を観測するために，ハニーポットとして X-POT を用いている．

上述したハニーポット以外にも，IoT 機器の実機を用いたハニーポットである IoT ポット[4]や，インフラの遠隔管理システムを模倣したハニーポット[5]など，様々な種類のハニーポットが提案されている[6].

マルウェアの Exploit 分析: マルウェアに含まれる Exploit の分析結果が報告されている[7] ．具体的には, マルウェアを動的解析環境で動作させ，TCP サーバと通信させることで, マルウェアがサーバに対して行う攻撃を観測している．結果として，マルウェアが様々な脆弱性を狙った攻撃を行うことが明らかとなっている．マルウェアライフサイクルの大規模調査[8]では，マルウェア解析の結果を整理しており，マルウェアが狙う脆弱性や機器を明らかにしている．

3. 提案アーキテクチャ

3.1 アーキテクチャ概要

提案アーキテクチャは，図 1 に示すように，ハニーポット，動的解析部，攻撃タグ付け部から構成される．ハニーポットで収集された検体は，動的解析にかけられ，動的解析の際の通信中に含まれる攻撃リクエストが抽出される．動的解析とハニーポットで直接得られた攻撃コードは，攻撃タグ付け部に渡され，既知の攻撃であれば，CVE 番号や攻撃対象の機器などのタグが付与される．具体的には，ハニーポットの観測データや動的解析の結果は Elasticsearch に記録されるようになっており, 攻撃のタグは Elasticsearch の一要素として記録されるようになっている．以下では，それぞれのコンポーネントについて述べる．

ⓒ2022 Information Processing Society of Japan

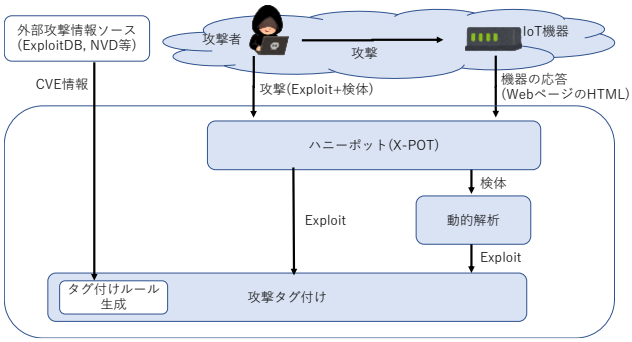

図 1　提案アーキテクチャ概要

3.2　ハニーポット

2 章で述べたように，本アーキテクチャはハニーポットに HTTP ハニーポットである X-POT を利用している. 本アーキテクチャでは, オリジナルの X-POT に以下の改良を加えている.

- 応答の優先度 : X-POT は, あるパスに複数の IoT 機器の応答が紐付けられている際には，優先度の高い応答を高い確率で返すようになっている．応答の優先度が高くなる条件として，オリジナルの X-POT では，応答を返した後に再度アクセスがあった際に，その応答に攻撃側が反応したと仮定して優先度を高くしていた．しかし，スキャン等で再アクセスがあった場合に不当に優先度が高くなる可能性があるため，実際に攻撃が行われ，検体の収集に寄与した応答の優先度を高くするように変更し，検体の収集の効率化を図った.
- ダウンローダーの対応 : X-POT は，観測したリクエストの中に wget や curl 等のコマンドにより検体のダウンロードが試みられている際には，その URL にアクセスし，マルウェアの検体をダウンロードする．取得した検体がダウンローダであった場合は，さらにダウンローダを解析して, ダウンローダの中の URL を抽出し，ダウンロードを試みるように拡張を行った．これを多重に行うことにより，ダウンローダが多重に用いられた際にも最終的にダウンロードされるマルウェア本体を収集可能である.
- 観測データの記録 : ハニーポットで観測された情報や検体の取得状況は，すべて Elasticsearch に格納するように拡張を行い，分析しやすいようにした.

3.3　動的解析部

動的解析部は，ハニーポットで収集した全検体に対して動的解析を行う(図 2)．解析環境の OS は Linux を想定し，CPU アーキテクチャとして，ARM, X86, MIPS に対応している．また，動的解析は，docker を用いて行い，ファイル操作やネットワーク通信を記録する．ネットワークに関して，pynetsim[10]を用いて，インターネットを仮想的にエミュレートしている．マルウェアはその種類によっては感染拡大のための攻撃機能があるものも存在する．よって，通信はすべてキャプチャされ，後述する攻撃タグ付け部によって，攻撃であればタグ付けがなされる．さらに，ハニーポットのデータと同様に，動的解析の結果も Elasticsearch に集約されるようになっている.

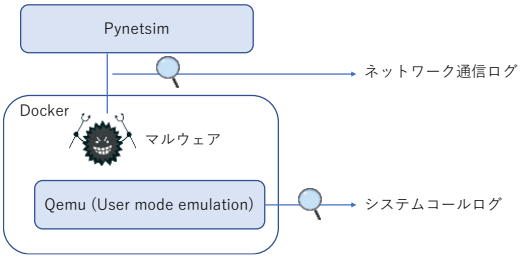

図 2 動的解析

3.4　攻撃タグ付け部

攻撃タグ付け部は，ハニーポットへのアクセスと，動的解析の通信に対して, 攻撃のタグ付けを行う(図 3). ハニーポットでは大量のイベントが観測されるため，すべてに対してタグ付けすることは難しい．具体的には，ハニーポットで観測されるイベントの多くはスキャンなどの Exploit ではない通信が大半を締めており，これを除外したい．従って，事前に攻撃か否かを判定して，明らかに攻撃と分かる通信だけを抽出しタグ付けを行う．また，タグ付けは，事前に定められたタグ付けルールに従って行われる．それぞれのステップについて，以下で詳しく述べる.

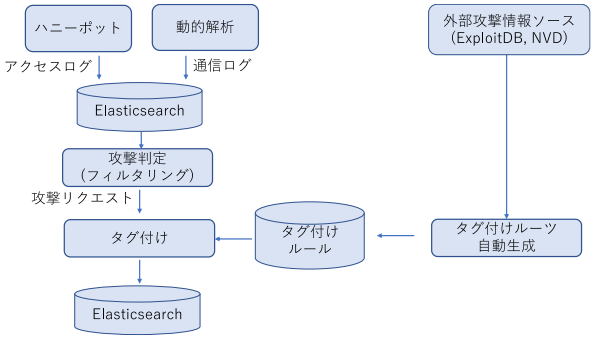

図 3 攻撃タグ付けの処理手順

3.4.1 攻撃判定

上述したように，ハニーポットでは大量のアクセス観測されており，そのすべてについてタグ付けを行うことは非効率である．そこで，攻撃と明らかに分かるイベントについてタグ付けを行っている.

現時点では, wget や curl などのマルウェアをダウンロードする目的としてよく利用されるコマンドが含まれる HTTP リクエストを攻撃としている．ただし，wget/curl が含まれない攻撃も多く，この部分の拡張は今後の課題である.

3.4.2 攻撃タグ付け

攻撃のタグ付けは，HTTP のリクエストのパスをベースに行われ, CVE 番号や攻撃対象の機器のタグが付与される.

また，攻撃のタグ付けは，事前に定めたルールに従って行われる．タグ付けのルールは，シグネチャとなる文字列と，タグから構成される．具体的には，1 つのルールは以下のように YAML 形式で記載される．

```
    condition:
    - '/dnslookup.cgi'
    memo: 'https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-
6334'
    tag: CVE-2017-6334
```

攻撃タグ付け機能は，HTTP のリクエスト中に，上述したルールの condition に記載された文字列が含まれるか否かを判定し，含まれる場合には，ルール中の tag に指定された文字列をタグとして付与する．上の例では，/dnslookup.cgi というパスへのアクセスに対して，CVE-2017-6334 というタグを付与する．

現時点では，116 件のタグ付けルールが登録されている．

3.4.3 攻撃タグ付けルールの自動生成

日々新しい脆弱性が報告され，それを悪用した攻撃が現れるため，手動で攻撃タグ付けルールを生成するのでは，運用のコストが大きい．そこで，本アーキテクチャでは，攻撃情報の公開データベースから情報を取得し，タグ付けルールを自動生成する．

具体的には，ハニーポットで観測された HTTP リクエストと動的解析で観測された HTTP リクエストのうち，攻撃と判定されたリクエストについて，タグ付けルールが存在ししているかを確認する．そして，タグ付けルールが存在しないリクエストについて，HTTP のリクエストのパスをベースに公開情報を検索し，一致するデータベースのエントリから CVE 番号や攻撃対象の機器を特定し，前節で述べた攻撃タグ付けルールを生成する．本手法の詳細は，論文[9]で述べる．

3.4.4 攻撃タグ付けのタイミング

攻撃のタグ付けは，攻撃タグ付けルールがアップデートされたタイミングで行われる．さらに，定期的にバッチ処理で新しく取得したハニーポットや動的解析のデータに対してタグ付けを行う．

3.1 データ保存と解析

ハニーポットの観測データやハニーポットで収集した検体の動的解析の結果は，すべて Elasticsearch に記録されるようになっている．また，攻撃タグ付け部が付与するタグも，Elasticsearch の各データの要素として関連付けて記録されている．

Elasticsearch に記録されたデータの解析に関して，Elasticsearch の可視化ツールである Kibana や，Python で Elasticsearch から必要なデータを取り出して分析を行う．

4. 解析結果

4.1 データセット

ハニーポットの 22 インスタンスで 2021 年 1 月 1 日から 2022 年 2 月末までに収集したデータを解析した．HTTP アクセスは計 4800 万件であり，ユニークな 33 万 IP アドレスからのアクセスを観測した．その内，70 万件のアクセスに対して CVE もしくは攻撃対象の機器のタグ付けが行われた．また，付与されたタグの種類は計 50 種類(詳しくは，付録の表 1 を参照)であった．一方，タグ付けルールが存在せずにタグが付けられなかった件数は 23272 件であった．

また，動的解析ついては，上記期間に収集した 6297 件のユニークな検体を用いた．

なお，ハニーポットの観測データや検体の一部は，筆者らの Web サイト[a]で研究組織向けに提供を行っている．

4.1.1 観測期間中の Exploit の動向

動的解析の結果，各検体に含まれる Exploit と検体が収集された時期を図 4 に示す．データが無い時期は，動的解析システムの運用の停止をしていた期間である．検体が収集された時期に応じて，動的解析時に観測される Exploit に差があることが分かる．また，ハニーポットで観測された攻撃について，そのトレンドを図 5 に示す．こちらも，時期によって利用される脆弱性に違いがあることが分かる．

ハニーポットでの観測と，検体の収集時期とを比較すると必ずしも一致していない．これは，ハニーポットが観測する攻撃は，マルウェアが行うものと，攻撃者が用意したサーバが行うものの両方が観測されているためであると考えられる．

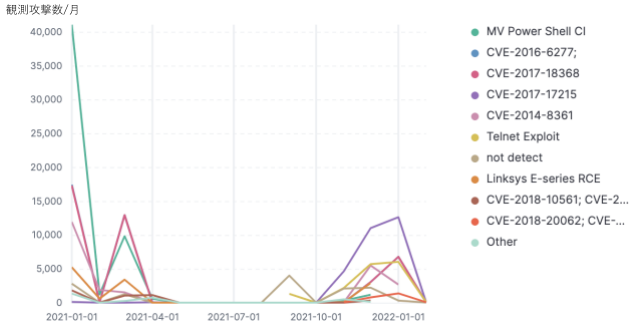

図 4 動的解析で観測された Exploit と検体収集時期

a 横浜国立大学 検体提供ページ．https://sec.ynu.codes/iot

ⓒ2022 Information Processing Society of Japan

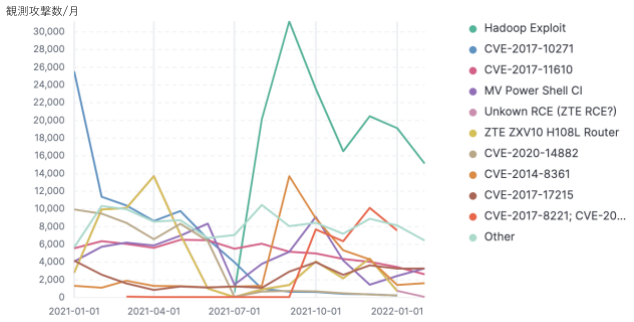

図 5　ハニーポットで観測された攻撃

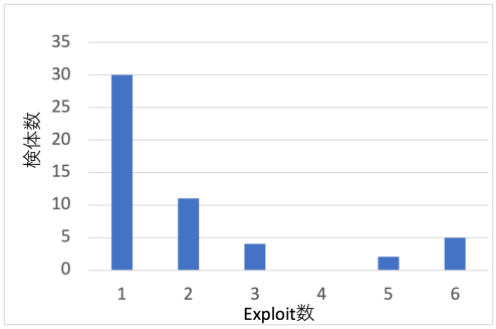

図 7　マルウェア検体が持つ Exploit 数

4.1.2 攻撃に利用されている脆弱性の公開日

動的解析で観測された攻撃とハニーポットで観測された攻撃について CVE 番号が判明しているものについて，CVE が登録された年を調査した．結果を図 6 に示す．動的解析とハニーポットで観測された攻撃は，両方とも古い脆弱性から新しい脆弱性まで，幅広く攻撃に利用されていることがわかる．

また，動的解析中にマルウェアが行った攻撃の対象の CVE とハニーポットで観測された攻撃対象の CVE の関係を分析したところ，ハニーポットを用いた観測の方が数が多く，動的解析で観測した攻撃対象の CVE は，2 件を除いてハニーポットでも観測されていた．また，ハニーポットのみで観測された 18 件の攻撃対象の CVE のうち，13 件は IoT 機器の脆弱性であった．従って，IoT 機器に対する攻撃の全体像を明らかにするためには動的解析での調査[11]では不十分であり，ハニーポットでの観測も重要であるといえる．

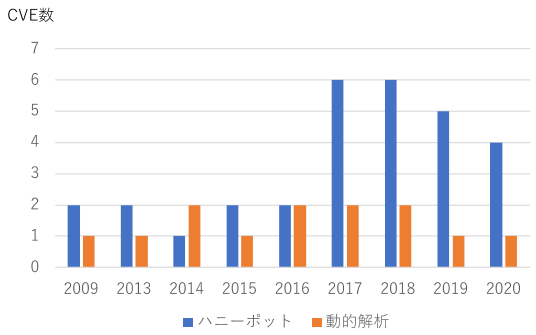

図 6　攻撃対象の脆弱性の CVE 登録年

4.1.3 検体に含まれる Exploit の件数

動的解析で観測した Exploit について，各検体が何種類の Exploit 用いて攻撃を行った分析した．大半は，1 つの Exploit であるが，中には，5 個や 6 個の Exploit を持つ検体も確認できた(図 7)．

5.　アーキテクチャ改良とデータ解析方針

5.1　アーキテクチャの改良

上記のプロトタイプを用いた評価によって，いくつかの改良点が明らかになった．ここでは問題点とその改善策について述べる．

攻撃タグ付け対象の拡大：3 章で述べたように，現在は明らかに攻撃と分かるイベントのみを抽出し，CVE 番号や攻撃対象の機器のタグ付けを行っている．よって，その条件を満たさない攻撃についてはタグが付いていない．これを改善するために，2 つのアプローチを検討している．1 つめのアプローチは，処理速度を高めることで，攻撃か否かを判定せず，すべてのデータをタグ付けの対象とすることである．現在のタグ付けは，Python の 1 プロセスだけで動作しているため，これをマルチスレッド化することで高速化が見込める．もしくは，データを Elasticsearch から取り出してからタグ付けし，Elasticsearch に書き戻しているので，Elasticsearch の script query を用いて Elasticsearch 内で処理を完結できれば高速化が見込める．2 つめのアプローチは，攻撃と判定するロジックの改良である．上述したように現在は curl/wget が入っているもののみを攻撃と見なしているが，攻撃の取りこぼしがないようにパターンを増やすことを検討する．

タグ付けルールの高度化：現在のタグ付けは，基本的に HTTP のパスを元に行っている．これは，攻撃対象の脆弱性が HTTP のパスと一致する場合が多いためである．しかし，ハニーポットの観測データを精査したところ，以下のようにランダムな文字列がパスとなっている場合があることが分かった．

/Xh7f	/mOQO	/0fcc	/TSpF	/JJsV	/LkVO

このような場合でも，タグ付けを効率的に行えるように，ワイルドカードや正規表現によってタグ付けルールを記述できるように改良を行いたい．

また，このようなランダムなパスへのアクセスは，そもそも発見しにくいという課題がある．解析の優先度として，パスごとにアクセス数を集計して，数の多いパスから解析を行っているため，このようにランダムな 4 文字のような

ⓒ2022 Information Processing Society of Japan

アクセスパターンの場合は，集計上の数が少ないように見え，優先度が下がってしまう．このようにランダムな文字列が含まれる場合でも，パターン認識などの技術を用いて効率的に攻撃をグループ化し，タグ付けを効率的に行えるようにする予定である．

X-POT 以外のハニーポットのデータ解析：筆者らは，HTTP ハニーポットである X-POT 以外に，IoT 機器の実機を用いた Telnet ハニーポットである IoTPOT を運用している．IoTPOT についてもデータは Elasticsearch に集約されるようになっているため，今後はこのデータも解析の対象とする予定である．

5.2 データ解析

ゼロデイ脆弱性の発見に向けた戦略：

2 章で述べたように，X-POT は模倣する機器を拡張することができるため，特定の機器を狙った攻撃も観測可能である．よって，まだ報告されていないゼロデイ脆弱性を利用した攻撃をいち早く観測できる可能性がある．しかし，ゼロデイ脆弱性を狙った攻撃を大量の観測データから見つけ出すためには，既知の攻撃をすべてタグ付けし，タグ付けがされなかった攻撃を精査する必要がある．よって，今後，タグ付けルールを拡張することで，未知の攻撃をあぶり出し，ゼロデイ脆弱性の発見につなげたい．

ハニーポットの観測と動的解析の統合解析：

前章では，ハニーポットの観測データと，動的解析の観測データの統計的な分析の例を示した．一方，本アーキテクチャは，ハニーポットへの Exploit，検体のダウンロード，検体の動作，検体のネットワークへの攻撃の 1 サイクルのすべてのデータを関連付けて処理可能であり，個々の攻撃キャンペーンの詳細をより詳しく分析可能であると考えている．このような観点から，攻撃の実態を明らかにしたい．

6. 結論

本論文では，ハニーポット，動的解析，ルールベースの攻撃タグ付けを組み合わせ，攻撃観測と分析を統合したアーキテクチャを提案した．プロトタイプを実装し評価実験を行った結果，50 件を超える脆弱性を狙う攻撃がハニーポットで観測されていることが明らかになった．加えて，動的解析中にマルウェアが行った攻撃の対象の CVE とハニーポットで観測された攻撃対象の CVE の関係を分析したところ，動的解析で観測した攻撃の 85%はハニーポットでも観測されていた．今後は，アーキテクチャの機能を拡張し，より詳細な分析を行う予定である．

謝辞 本研究は総務省の「電波資源拡大のための研究開発(JPJ000254)」における委託研究「電波の有効利用のための IoT マルウェア無害化／無機能化技術等に関する研究開発」によって実施した成果を含む．

参考文献

[1]Manos Antonakakis et.al., Understanding the Mirai Botnet, Usenix Security’17

[2]サイバーセキュリティタスクフォース事務局，サイバー攻撃の最近の動向等について,2022

[3]Seiya Kato, Rui Tanabe, Katsunari Yoshioka, Tsutomu Matsumoto, "Adaptive Observation of Emerging Cyber Attacks targeting Various IoT Devices," IFIP/IEEE International Symposium on Integrated Network Management (IM), 2021.

[4]Yin Minn Pa Pa, Suzuki Shogo, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow "IoTPOT: A Novel Honeypot for Revealing Current IoT Threats," Journal of Information Processing, Vol. 57, No. 4, 2016.

[5]Takayuki Sasaki, Akira Fujita, Carlos Hernandez Ganan, Michel van Eeten, Katsunari Yoshioka, Tsutomu Matsumoto, "Exposed Infrastructures: Discovery, Attacks and Remediation of Insecure ICS Remote Management Devices," Proc. 43rd IEEE Symposium on Security and Privacy (IEEE S&P), 2022.

[6]J. Franco, A. Aris, B. Canberk and A. S. Uluagac, "A Survey of Honeypots and Honeynets for Internet of Things, Industrial Internet of Things, and Cyber-Physical Systems," in IEEE Communications Surveys & Tutorials, vol. 23, no. 4, pp. 2351-2383, 2021

[7]鮫嶋海地，佐々木貴之，田辺瑠偉，吉岡克成，中尾康二，松本　勉, "IoT マルウェアが狙う脆弱性の変遷の動的解析による分析," 電子情報通信学会情報システムセキュリティ研究会, 2021.

[8]Omar Alrawi, Charles Lever, Kevin Valakuzhy, Ryan Court, Kevin Snow, Fabian Monrose, Manos Antonakakis, The Circle Of Life: A Large-Scale Study of The IoT Malware Lifecycle, Usenix Security’21

[9]九鬼琉，植田岳洋，佐々木貴之，吉岡克成，松本勉，ハニーポットで観測されたサイバー攻撃の対象機器及び脆弱性の自動推定手法の提案，第 97 回 CSEC 研究発表会, 2022

[10] PyNetSIm, https://github.com/jjo-sec/pynetsim

[11]Arwa Abdulkarim Al Alsadi, Kaichi Sameshima, Jakob Bleier, Katsunari Yoshioka, Martina Lindorfer, Michel van Eeten, Carlos H. Ganan, "No Spring Chicken: Quantifying the Lifespan of Exploits in IoT Malware Using Static and Dynamic Analysis," The 17th ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2022), 2022

ⓒ2022 Information Processing Society of Japan

付録

表 1　ハニーポットで観測した攻撃一覧

CVE/攻撃対象機器	観測回数	CVE/攻撃対象機器	観測回数
Hadoop Exploit	146682	CVE-2019-12780	1240
CVE-2017-10271	79598	Vacron NVR RCE	1026
CVE-2017-11610	72767	Linksys E-series RCE	742
MV Power Shell CI	68120	LILIN DVR 0-day	700
Unkown RCE (ZTE RCE?)	58601	Eir Exploit	498
ZTE ZXV10 H108L Router	58289	CVE-2016-10372	495
CVE-2020-14882	52357	CVE-2018-20062; CVE-2019-9082	178
CVE-2014-8361	45942	CVE-2018-7600	175
CVE-2017-17215	33569	CVE-2020-9054	171
CVE-2017-8221 CVE-2017-8222 CVE-2017-8223 CVE-2017-8224 CVE-2017-8225	31837	OptiLink Exploit	141
CVE-2018-14933	19110	CVE-2020-5722	97
NUUO NVRmini RCE	19110	CVE-2020-8515	96
CVE-2019-16920	15059	CVE-2017-14135	62
Unkonwn RCE (Docker?)	13431	SonicWall GMS-XMLRPC CI	55
CVE-2018-10561 CVE-2018-10562	7906	Netlink GPON RCE	45
CVE-2009-5157	7751	CVE-2009-0545 CVE-2019-12725	33
Netgear DGN1000 RCE	7748	CVE-2019-19356	28
CVE-2016-6277;	7256	CVE-2013-7179	15
CVE-2015-2051	6166	CVE-2017-18368	14
ADB Exploit	5641	D-Link DSL-2750B OS CI	14
Multi-vendor CCTV/DVR RCE	3995	Sar2HTML Exploit	6
CVE-2013-7471	3980	CVE-2019-19824	5
AVTECH Exploit	3076	CVE-2018-17173	1
AVTECH IPCam	2251	CVE-2018-20841	1
CVE-2015-1427	1265	CVE-2019-7256	1
		不明(タグ付けルール未作成の攻撃)	23272

ⓒ2022 Information Processing Society of Japan