6ZC-01

ビルシステムにおけるセキュリティ訓練ツールの提案

華原　依博†　　加藤　雅彦†　　小林　信博†
長崎県立大学†

1. はじめに

情報化された現代の社会において、統合 IP ネットワークで管理されたビルシステムが普及しつつあるが、ビルシステムの内部には多くのネットワーク機器や IoT 機器が存在しており、Mirai 等の IoT マルウェアがビル全体に悪影響を及ぼす可能性は十分予見される。そのため、この問題に対する防衛策の適切な運用が安全なビルシステム構築のための急務となっている。また、セキュリティインシデントへの対応が遅れたために被害が拡大した前例も存在するため、セキュリティ担当者の習熟のために IoT マルウェアに侵入された前提での訓練も必要である。

本研究では、ビルシステム内に IoT マルウェアが侵入した前提での訓練ツールを提案する。特に、Mirai の通信機能・増殖機能に着目し、ビルシステム内に Mirai に感染した機器である bot の実機を設置し、仮想環境上に bot に対する命令を行う CnC サーバと新たな機器へマルウェアのダウンロードを行う loader を設置することにより、安全な訓練環境とシナリオを作成する。その上で、訓練環境上でシナリオの一連の流れの自動化を行い、従来困難であった実際のビルシステムに近い本番環境上でセキュリティインシデントを再現した対応の訓練を可能とする。

1.1. IoT マルウェア Mirai

現在インターネット上には多くの種類の IoT マルウェアが存在しているが、その中でも Mirai は 2016 年 8 月に最初に発見され、様々なサービスに対して DDoS 攻撃を行い大きな注目を浴びた。

Mirai の増殖機能は、まず感染した機器である bot が、他に感染可能な機器が無いかランダムな IP アドレスに対してネットワークのスキャンを行う。次に Loader が、このスキャン結果の情報を基に新たな感染先に Mirai をダウンロードし起動することで多数の bot からなる botnet を構築する。そして、CnC サーバが botnet に対して命令を行うことで指定した攻撃対象に対して大規模な DDoS 攻撃を行う。

A proposal for security training tools in Building Systems
†Yorihiro Kahara, Nobuhiro Kobayashi
†University of Nagasaki

2. 提案手法

本研究では、セキュリティインシデントが発生した際にセキュリティ担当者が迅速に対応できるよう習熟することが目的である。そのために、Mirai がビルシステム内に既に侵入している前提の訓練環境とシナリオを作成し、訓練ツールを用いてシナリオを自動的に実行する。

2.1. 訓練環境について

本来、CnC サーバと Loader はビルシステム外部のインターネット上に存在しているが、不正アクセス禁止法を踏まえて安全を期すため、仮想環境上に外部ネットワークと遮断された疑似外部ネットワークを用意し、その中に CnC サーバ群を設置する。また、ビルシステム内に Mirai に感染した bot に相当する IoT 機器の実機(Raspberry Pi 4)を設置する(図 1)。これにより、疑似外部ネットワークによる安全性と IoT 機器の実機によるマルウェアの動作の再現保証を両立したハイブリッド型の訓練環境が実現できる。

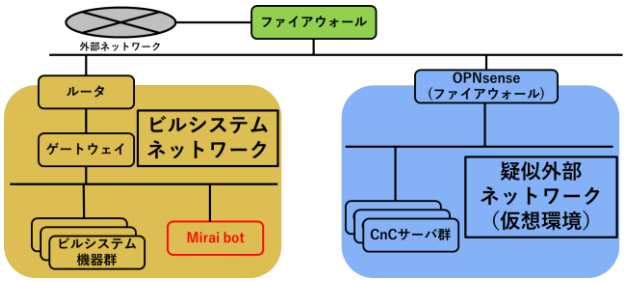

図1 訓練環境のネットワーク構成

2.2. 訓練シナリオ

本研究では、セキュリティインシデントを再現した対応の訓練を行うため Mirai の通信機能・増殖機能に着目し、3 種類のシナリオを提案する。各シナリオの Mirai のネットワークにおける適用範囲を図 2 を用いて説明する。

①シナリオ 1

・既にビルシステム内部の機器が Mirai に感染し、bot が起動している状態
・bot が CnC サーバと通信を確立した状態

②シナリオ 2

・bot がネットワークをスキャンしている状態

・スキャンで取得した新たな感染先の認証情報を抽出・整形し、SSH プロトコル経由で Loader に送信を行う状態

③シナリオ 3

・bot が CnC サーバから攻撃命令を受け取る状態
・命令を受け取った bot が攻撃対象のサーバに対する攻撃を開始する状態

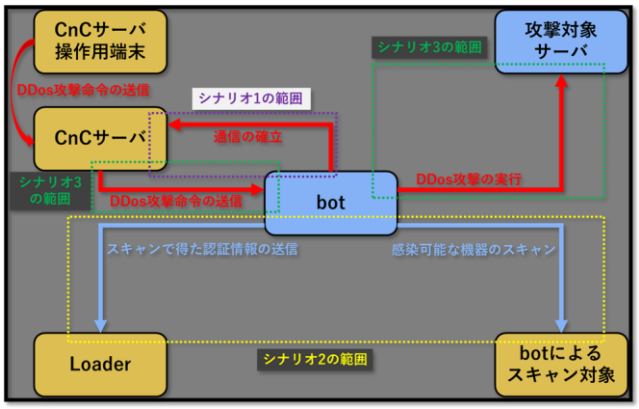

図 2 Mirai のネットワークにおける
各シナリオの適用範囲

3. 訓練ツール

各シナリオを自動化し Mirai の動作を再現する訓練ツールを、シェルスクリプトとして実装した。更に、Mirai の通信機能が再現されていることを、通信パケットのキャプチャで確認した。

シナリオ１：scenario1.sh, cnc_start.sh 他
シナリオ２：scenario2.sh, scanner.sh
シナリオ３：scenario3.sh, start_attack.sh

4. 評価

本研究は、セキュリティ対策としてビルシステム内に NIDS が設置されていることを想定した評価を行った。例として、シナリオ 1 において bot が CnC サーバと行う生存確認（Heartbeat）の通信を NIDS の snort により検知[1]し、出力されたアラートをセキュリティ担当者が確認する訓練を行った。訓練の結果、図 3 に示す通り bot と CnC サーバの生存確認のパケットのやり取りが検知され、アラートが出力されることを確認した。これは、訓練ツールにより Mirai の動作が再現され、ビルシステムのセキュリティ対策が機能しセキュリティ担当者の対応につながったことを意味する。従って、訓練ツールが訓練に活用可能であると判断する。

```
[**] [1:1000001:1] Mirai Botnet: Send Heartbeat from Bot to C&C [**]
[Priority: 0]
12/15-17:58:42.166328 192.168.250.210:23 -> 192.168.62.154:38152
TCP TTL:62 TOS:0x0 ID:40563 IpLen:20 DgmLen:54 DF
***AP*** Seq: 0x3977897E  Ack: 0xB3799376  Win: 0xE3  TcpLen: 32
TCP Options (3) => NOP NOP TS: 2209325929 3589648169

[**] [1:1000002:1] Mirai Botnet: Reply Heartbeat from C&C to Bot [**]
[Priority: 0]
12/15-17:59:42.210480 192.168.250.210:23 -> 192.168.62.154:38152
TCP TTL:62 TOS:0x0 ID:40567 IpLen:20 DgmLen:54 DF
***AP*** Seq: 0x39778980  Ack: 0xB3799378  Win: 0xE3  TcpLen: 32
TCP Options (3) => NOP NOP TS: 2209385968 3589708213
```

図 3 snort によるアラート の出力

5. 考察

5.1. 訓練シナリオについて

本研究では、Mirai の通信機能・増殖機能に着目し、ビルシステム内で想定される Mirai の感染拡大の訓練シナリオを 3 段階に分解した。これにより、それぞれのシナリオにおける Mirai の挙動に対して個別の対応の訓練を行うことが可能であり、セキュリティ対策の変更やセキュリティ担当者の交代が生じた際の習熟に貢献するものと考えられる。また、本研究で作成したシナリオをベースに拡張することで、新たな通信方式や増殖方法をとる Mirai の亜種や新種の IoT マルウェアに対応が可能と考えられる。

5.2. 訓練ツールについて

本研究では、bot に相当する IoT 機器の実機と仮想環境上の疑似外部ネットワークを組み合わせて、ビルシステムの本番環境上に Mirai の bot ネットを再現するとともに、シナリオを自動化する訓練ツールを作成した。これにより、実機での bot の動作の確実性（再現保証）と疑似外部ネットワークによる安全性を両立した訓練ツールを実現した。その結果、従来困難であった実際のビルシステムに近い本番環境上でセキュリティインシデントを再現し、対応の訓練を行えることが確認できた。

更に、新たなビルシステムでの訓練の際には、小型で運搬が可能な bot に相当する IoT 機器を設置し、疑似外部ネットワーク上に構築済の CnC サーバ群と接続することで、容易に実施が可能であり、幅広い活用が期待できる。

謝辞：本研究の実施にあたり、大成建設株式会社の方々には、ご協力及びご助言をいただきましたことを、深く感謝いたします。

参考文献

[1]IIJ.″Mirai Botnet Detection and Countermeasures″ . https://www.iij.ad.jp/en/dev/iir/pdf/iir_vo133_infra_EN.pdf（参照 2022-12-16）