Dr.WEB®
Anti-virus

あなたのTVが踏み台にされています！

株式会社Doctor Web Pacific

www.drweb.com

Dr.WEB®
Anti-virus

今回のテーマ

- Android TV が狙われています！
- DDoS攻撃とは
- トロイの木馬「Mirai」

Dr.WEB®
Anti-virus

Android TVが狙われています！

www.drweb.com

Android TV が狙われている！

- 2023年9月7日にDoctor Web Pacific は、

  「開かれたパンドラの箱：悪名高い**トロイの木馬 Mirai** が
  新たな偽装でAndroid TVセットとTVボックスに侵入」

  というニュースを公表しました。

- Android OSの**ファームウェアの更新中**にトロイの木馬 Mirai に感染します。

- トロイの木馬 Mirai は、感染したデバイスにリモート制御されたボットのネットワークを作ります。
  このボットネットワークは**DDoS攻撃**に利用されます。

Dr.WEB®
Anti-virus

DDoS攻撃とは

DDoS攻撃とは

DDoS（Distributed Denial of Service）攻撃とは、攻撃対象となるWebサーバに対し、**複数のコンピューターから大量のパケットを送りつける**ことで、正常なサービス提供を妨げる行為を指します。

サーバが高負荷状態となり、レスポンスの低下・応答不能・ネットワークの輻輳などの弊害が起きます。

Dr.WEB®
Anti-virus

トロイの木馬
Mirai のねらい

トロイの木馬Miraiの攻撃ターゲット

Miraiのターゲット

Android TVデバイスを狙っている。

特に低価格帯のAndroid TV デバイスユーザーが危険

- Tanix TX6 TV Box
- MX10 Pro 6K
- H96 MAX X3

なぜ「パンドラの箱」なのか

ニュース：
開かれた**パンドラの箱**：悪名高いトロイの木馬 Mirai が新たな偽装でAndroid TVセットとTVボックスに侵入

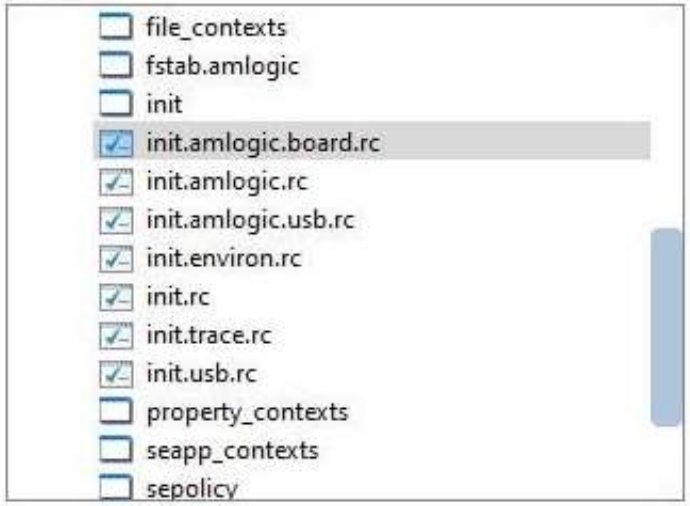
なぜ**パンドラの箱**なのか？
それは、systemディレクトリ内に **pandoraspearrk** というオブジェクトが存在したからです。

このファイルの目的は、バックドアを作られたデバイス自体を利用してDDoS攻撃を実行させることでした。

なぜダウンロードされるのか。

なぜ、パンドラファイルはダウンロードされるのか？

File List



Content

```
    disabled
    oneshot

# sowell add start
service hello_word /system/bin/HelloWorld
        class core
        user root
        group root
service htvsleep /system/bin/htvsleep
        class core
        user root
        group root
service pndoraspear /system/bin/pandoraspear
        class core
        user root
        group root

service preinstall /system/bin/preinstall.sh
```

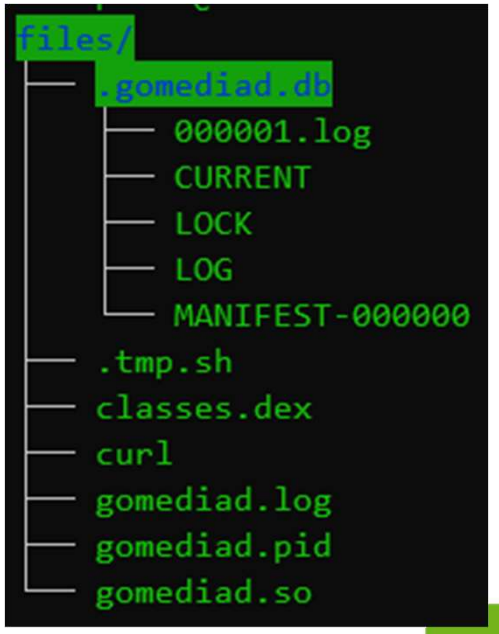
ファームウェア更新としてファイルが拡散されています。この更新は一般に公開されているAndroidオープンソースプロジェクトのテストキーで署名されているため、多くのサイトからダウンロード可能な状態になっていると考えられています。

感染後の動き

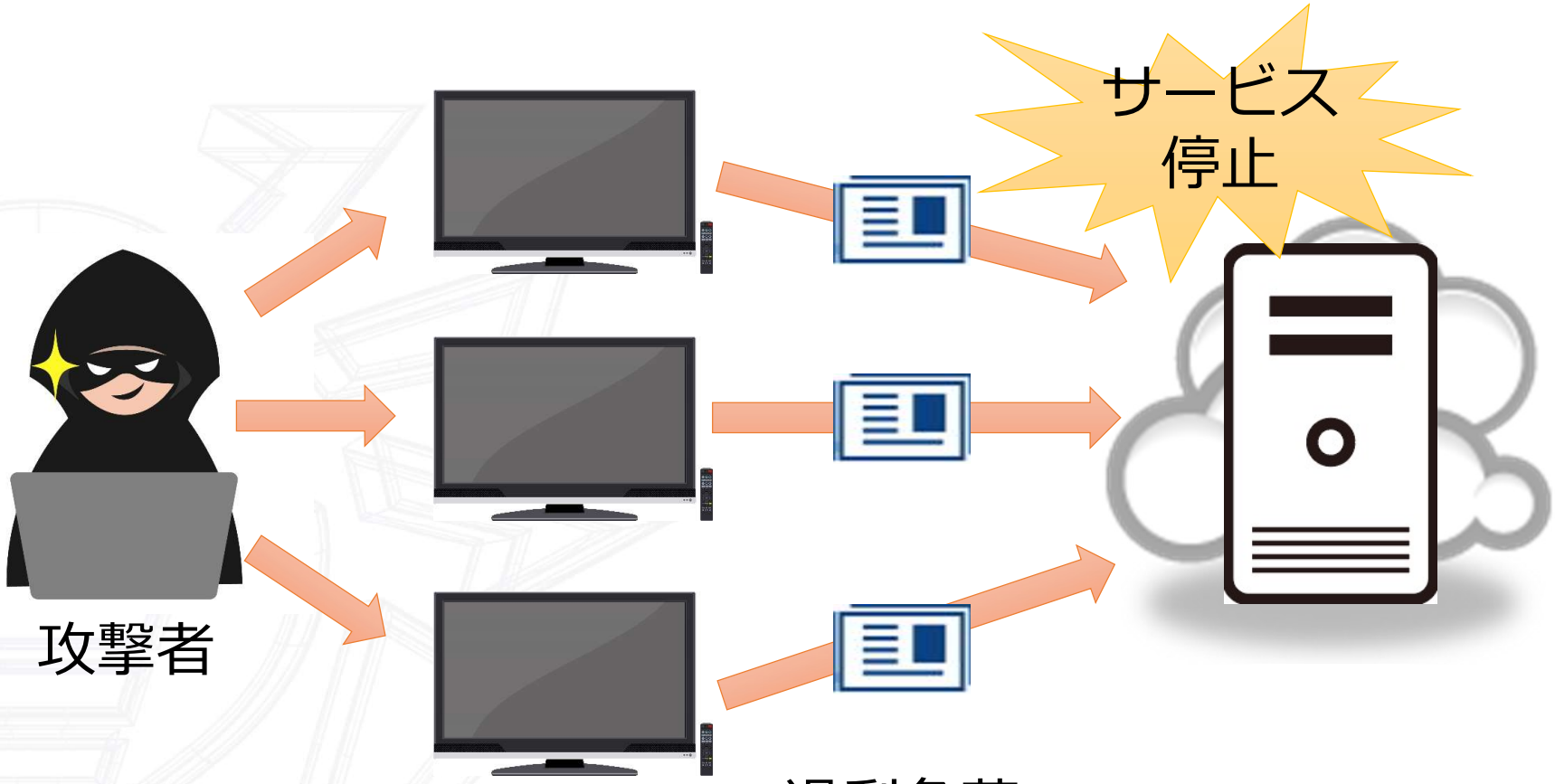
デバイスに感染すると、ユーザーに気づかれず密かにGoMediaServiceが開始されます。その後、デバイスの起動時にgomediad.soプログラムを呼び出し、複数のファイルが解凍されます。

画像はgomediad.soが起動後に作成するファイル構造になります。

ファイルが解凍されると**バックドアのインストーラが起動**され、攻撃者がTCPやUDPを介してDDoS攻撃を開始します。



Miraiに感染した Android TV



Dr.WEB®
Anti-virus

www.drweb.com
www.drweb.co.jp