Backdoorの調査と解析

task4233

学生エンジニアLT大会 #31

2019, 12/8

Who am I

Name

Takashi Mima(@task4233)

今までやってきたこと:

競プロ/CTF/Security Camp 2019 Aトラック

今やっていること:

マルウェア解析 / ペネトレのための学習と実践

taskCTF - Rainforest

シンワ測定 工事用 旗 ナイロン製 2本組 76909

★★★☆☆ 5

￥740 あわせ買い対象

価格が13%下がりました ほしい物リストに追加した時の価格は、￥855 でした

スタイル：ナイロン製

32点の新品/中古品 ￥686より

“*Do you wanna capture the flag? click here and show details.*
taskctf{Y0u_c4nn0t_5ee_the_f0re5t_f0r_the_tree5} ”

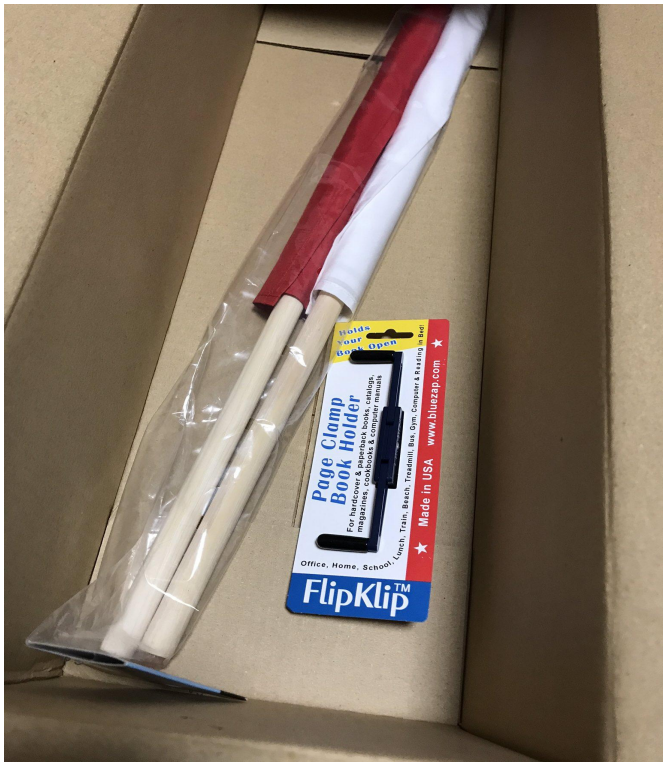
2019年12月2日に追加された商品

カートに入れる

移動 削除

コメント、数量、優先度を編集する

Capture the flag(物理)



もくじ

1. Backdoorとは

・コンピュータ内に設置する**裏口**

> 本来はIDやパスワードを使って使用権を確認する
> コンピュータの機能を**無許可で利用するため**に、
> コンピュータ内に(**他人に知られることなく**)
> 設けられた通信接続の機能 (ref: wikipedia)

もくじ

2. Backdoorの仕組み

・22/tcp, 25/tcp, 53/tcp, 53/udp, 80/tcp, 443/tcp等を
　利用して外部とのコネクションを作成
・22/tcp(ssh)
　- sshd_configの更新
　- rsa認証鍵の生成, 奪取

・80/tcp(http), 443/tcp(https)
　- cgiスクリプトの設定
　- 遠隔操作用の実行ファイル配置

ref: 攻撃者が侵入後に行うバックドアの設置例 (2002, atmarkit)

デモ

もくじ

Spidey Botの解析

・Spidey BotはDiscord ClientをBackdoor化するマルウェア

・マルウェア本体の検体が見つからなかったので情報をPOSTするJSを解析

ref :Discordにバックドアを仕掛けるマルウェアが発見 (2019 , 窓の社)
SPIDEY BOT TRANSMUTES WINDOWS DISCORD CLIENT INTO BACKDOOR (2019, SoCPrime)

Spidey Botの解析

・実際のコードと比較
- userinfo part
- timezone part
- resolution part
- ip part
- WebRTC ip part
- zoom part
- payment part
- version part
- clipboard part

- Discordのユーザートークン
- タイムゾーン
- 画面解像度
- ローカルIPアドレス
- WebRTC経由のパブリックIPアドレス
- ユーザー名/メールアドレス/電話番号など
- ズーム比
- 支払い情報
- Webブラウザのユーザーエージェント
- Discordのバージョン
- クリップボードの先頭から50文字

Any Question?

Spidey Botの検体を持っている方がいたらください

Twitter: @task4233
GitHub: task4233